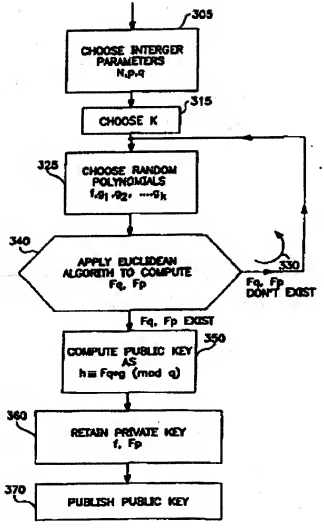
PUBLIC KEY CRYPTOSYSTEM METHOD AND APPARATUS

Publication number: JP2000516733T
Publication date: 2000-12-12
Inventor:
Applicant:
Classification:
- international: ***G09C1/00; H04L9/30;*** **G09C1/00; H04L9/28;** (IPC1-7): G09C1/00
- european: H04L9/30P
Application number: JP19980511051T 19970819
Priority number(s): WO1997US15826 19970819; US19960024133P 19960819

Also published as:
WO9808323 (A
EP0920753 (A1
EP0920753 (A0
CA2263588 (C)
AU716797 (B2)

Abstract not available for JP2000516733T
Abstract of corresponding document: **WO9808323**

This public-key cryptosystem endocing technique uses a mixing system based on polynomial algebra and recuction modulo two numbers while the decoding technique uses an unmixing system whose validity depends on elementary probability theory. A method for encoding and decoding a digital message comprises the steps: selecting ideals p and q of a ring R (305); generating elements f and g of the ring R (325), and generating an element F sub q which is an inverse of f (mod q), and generating F sub p which is an inverse of f (mod p) (340); producing a public key that includes h (350), where h is congruent, mod q, to a product that can be derived using g and F sub q; producing a private key from which f and F sub p can be derived; producing an encoded message by encoding the message using the public key and a random element; and producing a decoded message by decoding the encoded message using the private key.



(19)日本国特許庁（ＪＰ）　(12)公表特許公報（Ａ）　(11)特許出願公表番号
特表2000－516733
（P2000－516733A）
(43)公表日　平成12年12月12日(2000.12.12)

(51)Int.Cl.⁷	識別記号	ＦＩ	テーマコード（参考）
Ｇ０９Ｃ　1/00	６２０	Ｇ０９Ｃ　1/00	６２０Ａ

審査請求　未請求　予備審査請求　有　（全 69 頁）

(21)出願番号　特願平10－511051
(86)（22)出願日　平成９年８月19日(1997.8.19)
(85)翻訳文提出日　平成11年２月19日(1999.2.19)
(86)国際出願番号　ＰＣＴ／ＵＳ９７／１５８２６
(87)国際公開番号　ＷＯ９８／０８３２３
(87)国際公開日　平成10年２月26日(1998.2.26)
(31)優先権主張番号　６０／０２４，１３３
(32)優先日　平成８年８月19日(1996.8.19)
(33)優先権主張国　米国（ＵＳ）
(81)指定国　ＥＰ(ＡＴ，ＢＥ，ＣＨ，ＤＥ，ＤＫ，ＥＳ，ＦＩ，ＦＲ，ＧＢ，ＧＲ，ＩＥ，ＩＴ，ＬＵ，ＭＣ，ＮＬ，ＰＴ，ＳＥ)，ＡＵ，ＣＡ，ＣＮ，ＩＬ，ＪＰ

(71)出願人　エヌティーアールユー　クリプトシステムズ，インコーポレーテッド
アメリカ合衆国，ロード　アイランド　02860，ポータケット，レスター　ウェイ，３番地
(72)発明者　ホフスタイン　ジェフリー
アメリカ合衆国，ロード　アイランド　02860，ポータケット，レスター　ウェイ，３番地
(74)代理人　弁理士　山本　恵一

最終頁に続く

(54)【発明の名称】　公開鍵暗号システム方法および装置

(57)【要約】
この公開鍵暗号システム符号化技法は、２つの数を法とする多項式代数および整約に基づく混合システムを使用し、それに対して、復号技法は、妥当性が基本確率理論に依存する非混合システムを使用する。デジタル・メッセージを符号化し復号する方法は、乗Ｒのイデアルｐおよびｑを選択するステップ（３０５）と、乗Ｒの要素ｆおよびｇを生成するステップ（３２５）と、Ｆ　ｓｕｂ　ｑ，すなわち、ｆ（ｍｏｄ　ｑ）の逆数を生成するステップと、Ｆ　ｓｕｂ　ｐ，すなわちｆ（ｍｏｄ　ｐ）の逆数を生成するステップ（３４０）と、ｇおよびＦ　ｓｕｂ　ｑを使用して導出することのできる積と、ｑを法として合同であるｈを含む公開鍵を作成するステップ（３５０）と、ｆおよびＦ　ｓｕｂ　ｐを導出することのできる専用鍵を作成するステップと、公開鍵およびランダム要素を使用してメッセージを符号化することによって符号化メッセージを作成するステップと、専用鍵を使用して符号化メッセージを復号することによって復号メッセージを作成するステップとを含む。

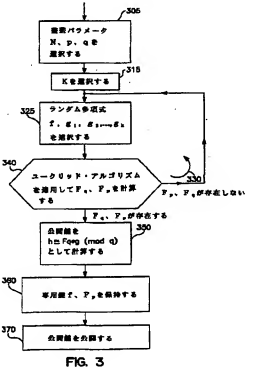


FIG. 3

【特許請求の範囲】

１．デジタル・メッセージｍを符号化し復号する方法であって、

環Ｒのイデアルｐおよびｑを選択するステップと、

環Ｒの要素ｆおよびｇを生成し、ｆ（ｍｏｄ　ｑ）の逆数である要素F_qを生成し、ｆ（ｍｏｄ　ｐ）の逆数である要素F_pを生成するステップと、

ｇおよびF_qを使用して得ることのできる積とｍｏｄ　ｑで合同であるｈを含む公開鍵を生成するステップと、

ｆおよびF_pを得ることのできる専用鍵を生成するステップと、

専用鍵およびランダム要素φを使用してメッセージｍを符号化することによって符号化メッセージｅを生成するステップと、

専用鍵を使用して符号化メッセージｅを復号することによって復号メッセージを生成するステップと

を含む方法。

２．前記環Ｒが環Ｚを覆うモジュールであることを特徴とする請求の範囲第１項に記載の方法。

３．Ｚを覆うＲの次元がＮであり、Ｎが１より大きな整数であることを特徴とする請求の範囲第１項に記載の方法。

４．環Ｒが、特定の多項式を法とする多項式の環であることを特徴とする請求の範囲第３項に記載の方法。

５．要素を生成する前記ステップがさらに、ｇ（ｍｏｄ　ｑ）の逆数である要素G_qを生成し、ｇ（ｍｏｄ　ｐ）の逆数である要素G_pを生成するステップを含むことを特徴とする請求の範囲第１項に記載の方法。

６．前記要素G_qが前記公開鍵を得るのに使用され、前記要素G_pが前記専用鍵の一部であることを特徴とする請求の範囲第５項に記載の方法。

７．前記選択ステップがさらに正の整数Ｋを選択するステップを含み、前記要素ｇがg_i（ｉ＝１，２，．．．．Ｋ）を含み、前記公開鍵ｈがh_i（ｉ＝１，２，．．．．Ｋ）を含むことを特徴とする請求の範囲第１項に記載の方法。

８．前記ランダム要素φがイデアルｐ中にφｉ（ｉ＝１，２，．．．．Ｋ）を含み、前

記符号化メッセージが、

$$e \equiv \sum_{i=1}^{k} \phi_i * h_i + m \pmod{q}$$

として生成されることを特徴とする請求の範囲第７項に記載の方法。

９．前記公開鍵および専用鍵がそれぞれ、ｐとｑをふくむことを特徴とする請求の範囲第１項に記載の方法。

１０．前記イデアルｐとｑが相対的に素な整数によって生成されることを特徴とする請求の範囲第１項に記載の方法。

１１．符号化メッセージが、メッセージｍと、φおよびｈを含む積

との和とｍｏｄ　ｑで合同であることを特徴とする請求の範囲第１０項に記載の方法。

１２．前記整数ｐとｑが等しくなく、ｐとｑがともに１より大きいことを特徴とする請求の範囲第１０項に記載の方法。

１３．前記符号化メッセージが、あるユーザによってある場所で生成され、前記ある場所から別の場所に伝送され、前記別の場所であるユーザによって復号されることを特徴とする請求の範囲第１項に記載の方法。

１４．デジタル・メッセージｍを符号化し復号する方法であって、

整数ｐおよびｑを選択するステップと、

多項式ｆおよびｇを生成するステップと、

逆数F_qおよび逆数F_pを決定するステップであって、

$$F_q * f \equiv 1 \pmod{q}$$

$$F_p * f \equiv 1 \pmod{p}$$

であるステップと、

ｐ、ｑ、ｈを含む公開鍵を生成するステップであって、

$$h \equiv F_q * g \pmod{q}$$

であるステップと、

ｆおよびF_pを含む専用鍵を生成するステップと、

専用鍵およびランダム要素φを使用してメッセージｍを符号化することによっ

て符号化メッセージｅを生成するステップと、

専用鍵を使用して符号化メッセージｅを復号することによって復号メッセージを生成するステップと

を含む方法。

１５．前記符号化メッセージｅが、

$$e \equiv p\phi^{*}h+m \pmod{q}$$

として生成されることを特徴とする請求の範囲第１４項に記載の方法。

１６．前記復号メッセージが、

$$a \equiv f^{*}e \pmod{q}$$

を計算し、ついで復号メッセージm'を

$$m' \equiv F_{p}^{*}a \pmod{p}$$

として計算することによって生成されることを特徴とする請求の範囲第１５項に記載の方法。

１７．多項式ｆおよびｇを生成する前記ステップが、正の整数Ｋを選択し、Ｋ個の多項式ｇを$g_1, g_2, \ldots, g_K$として生成するステップを含み、前記公開鍵が$h_1, h_2, \ldots, h_K$を含み、

上式で

$$h_i \equiv F_q^{*}g_i \pmod{q},\ i=1, 2, \ldots, K$$

であることを特徴とする請求の範囲第１４項に記載の方法。

１８．前記符号化メッセージｅが、

$$e \equiv p\phi_1^{*}h_1+p\phi_2^{*}h_2+\ldots+p\phi_K^{*}h_K+m \pmod{q}$$

として生成され、

上式で$\phi_1, \phi_2, \ldots, \phi_K$がＫ個のランダム多項式であることを特徴とする請求の範囲第１７項に記載の方法。

１９．前記符号化メッセージが、あるユーザによってある場所で生成され、前記ある場所から別の場所に伝送され、前記別の場所であるユーザによって復号されることを特徴とする請求の範囲第１４項に記載の方法。

２０．モニック多項式Ｍ（Ｘ）が選択され、多項式の乗算が、まず多項式の通常の乗算を行い、次いで結果をＭ（Ｘ）で割り、剰余だけを保持することによって実施されることを特徴とする請求の範囲第１４項に記載の方法。

２１．非ゼロの整数Ｎが選択され、多項式の乗算が、Ｎを法とする指数を整約することによって実施されることを特徴とする請求の範囲第１４項に記載の方法。

２２．前記多項式ｆ、ｇ、ｍ、φが有界係数をもつように制約されることを特徴とする請求の範囲第１４項に記載の方法。

２３．前記整数ｑが、前記整数ｐと、前記多項式ｆ、ｇ、ｍ、φの次数と、前記ｆ、ｇ、ｍ、φの係数に対する前記制約とによって決まる量よりも小さく選ばれることを特徴とする請求の範囲第２２項に記載の方法。

２４．前記整数ｑが、前記整数ｐと、前記多項式ｆ、ｇ、ｍ、φの次数と、前記ｆ、ｇ、ｍ、φの係数に対する前記制約とによって決まる量よりも大きく選ばれることを特徴とする請求の範囲第２２項

に記載の方法。

２５．デジタル・メッセージを符号化し復号する方法であって、

相対的に素な整数ｐおよびｑを選択するステップと、

非ゼロの整数Ｋを選択するステップと、

整数係数を有し、$w_i \equiv 0 \pmod{p}$．（ｉ＝１，２，...，Ｋ）である行列の環からＫ＋２個の行列ｆ，ｇ，g_1，w_2，...，w_Kを生成するステップと、

前記行列の環から逆行列F_p，F_q，G_p，G_qを生成するステップであって、

$$f F_p \equiv I \pmod{p}$$

$$f F_q \equiv I \pmod{q}$$

$$g G_p \equiv I \pmod{p}$$

$$g G_q \equiv I \pmod{q}$$

上式でＩが単位行列であるステップと、

公開鍵をＫ個の行列（h_1，h_2，...，h_k）のリストとして生成するステップであって、

$$h_i \equiv F_q w_i G_q \pmod{q},\ i = 1, 2, \ldots, K;$$

であるステップと、

専用鍵を行列（ｆ，ｇ，F_p，G_p）として生成するステップと、

専用鍵およびランダム整数ϕ_1，ϕ_2，...，ϕ_Kを使用してメッセージｍを符号化することによって符号化メッセージｅを

$$e \equiv \phi_1 h_1 + \phi_2 h_2 + \ldots + \phi_K h_K + m \pmod{q};$$

として生成するステップと、

$$a \equiv f e g \pmod{q}$$

および

$$b \equiv a \pmod{p}$$

を計算し、ついで復号メッセージｍ’を

$$m' = F_p b G_p \pmod{p}$$

として計算することによって復号メッセージｍ’を生成するステップと

を含む方法。

２６．前記符号化メッセージが、あるユーザによってある場所で生成され、前記ある場所から別の場所に伝送され、前記別の場所であるユーザによって復号されることを特徴とする請求の範囲第２５項に記載の方法。

２７．前記行列w_1，w_2，...，w_K，ｆ，ｇ，ｍが有界係数をもつように制約され、整数ϕ_1，ϕ_2，...，ϕ_Kが有界であるように制約されることを特徴とする請求の範囲第２５項に記載の方法。

２８．前記整数ｑが、前記整数ｐと、前記整数Ｋと、前記多項式w_1，w_2，...，w_K，ｆ，ｇ，ｍの次数と、前記多項式w_1，w_2，...，w_K，ｆ，ｇ，ｍの係数に対する前記制約と、整数ϕ_1，ϕ_2，...，ϕ_Kに対する前記制約とによって決まる量よりも小さく選ばれることを特徴とする請求の範囲第２７項に記載の方法。

２９．前記整数ｑが、前記整数ｐと、前記整数Ｋと、前記多項式w_1，w_2，...，w_K，ｆ，ｇ，ｍの次数と、前記多項式w_1，w_2，...，w_K，ｆ，ｇ，ｍの係数に対する前記制約と、整数ϕ_1，ϕ_2，...，ϕ_Kに対する前記制約とによって決まる量よりも大きく選ばれることを

特徴とする請求の範囲第２７項に記載の方法。

３０．デジタル・メッセージｍを符号化し復号するシステムであって、

イデアルｐおよびｑを選択する手段と、

環Ｒの要素ｆおよびｇを生成し、ｆ（ｍｏｄ　ｑ）の逆数である要素F_qを生成し、ｆ（ｍｏｄ　ｐ）の逆数である要素F_pを生成する手段と、

ｇおよびF_qを使用して得ることのできる積とｍｏｄ　ｑで合同であるｈを含む公開鍵を生成する手段と、

ｆおよびF_pを得ることのできる専用鍵を生成する手段と、

専用鍵およびランダム要素φを使用してメッセージｍを符号化することによって符号化メッセージｅを生成する手段と、

専用鍵を使用して符号化メッセージｅを復号することによって復号メッセージを生成する手段と

を備えるシステム。

３１．前記符号化メッセージが、あるユーザによってある場所で生成され、前記ある場所から別の場所に伝送され、前記別の場所であるユーザによって復号されることを特徴とする請求の範囲第３０項に記載のシステム。

３２．通信システムのユーザ間で情報を通信する方法であって、

リングＲと、Ｒ中のイデアルＰおよびＱと、イデアルＱを法とする環Ｒに対する代表剰余系C_Qの集合と、イデアルＰを法とする環Ｒに対する代表剰余系C_Pの集合とを生成するステップと、

Ｒ中の少なくとも２つの専用鍵要素$f_1,\ldots,f_n$および第１のユーザのイデアルＱの関数として環Ｒ中の少なくとも１つの公開鍵要素$h_1,\ldots,h_k$を生成するステップと、

環Ｒと、イデアルＱと、イデアルＰと、Ｒ中の要素$h_1,\ldots,h_k$との記述を第１のユーザから第２のユーザに伝送するステップと、

イデアルＰおよびＱと、公開鍵要素$h_1,\ldots,h_k$と、Ｒ中の専用メッセージ要素ｍと、第２のユーザの少なくとも１つの専用ランダム要素$\phi_1,\ldots,\phi_l$との関数として環Ｒ中の要素ｅを生成するステップと、

ｅ，ｆ$_1$，...，ｆ$_n$の関数Ｆを評価するＲ中の結果Ａを計算し、代表剰余系Ｃ$_Q$の集合中のＡの代表剰余系ａを計算し、ａ，ｆ$_1$，...，ｆ$_n$の関数Ｇを評価する結果Ｂを計算し、代表剰余系Ｃ$_P$の集合中のＢの代表剰余系ｂを計算し、ｂ，ｆ$_1$，...，ｆ$_n$の関数Ｈを評価する代表剰余系Ｃ$_P$の集合中の結果ｃを計算することによって、第１のユーザがメッセージ要素ｍを決定できるように、要素ｅを第２のユーザから第１のユーザに伝送するステップと

を含む方法。

３３．メッセージ要素ｍが、ｍがＣ$_P$の要素であるという条件を満たすことを特徴とする請求の範囲第３２項に記載の方法。

３４．ａ，ｂ，ｃ，ｆ$_1$，...，ｆ$_n$の関数を計算することによって、第１のユーザがメッセージ要素ｍを決定することを特徴とする請求の範囲第３２項に記載の方法。

３５．公開鍵要素ｈ$_1$，...，ｈ$_k$が、１とｋの間の各ｉについて要素ｆ$_1$がイデアルＱを法としてＲ中で積ｈ$_i$ ｆ$_{k+1}$と合同であるという

条件を満たすことを特徴とする請求の範囲第３２項に記載の方法。

３６．専用鍵要素ｆ$_1$，...，ｆ$_{k+1}$が、要素ｆ$_1$，...，ｆ$_k$がイデアルＰ中にあるという条件を満たすことを特徴とする請求の範囲第３２項に記載の方法。

３７．専用ランダム要素ϕ_1，...，ϕ_lがイデアルＰ中にあることを特徴とする請求の範囲第３２項に記載の方法。

３８．公開鍵要素ｈ$_1$，...，ｈ$_k$と、専用ランダム要素ϕ_1，...，ϕ_{k+1}と、専用メッセージ要素ｍとの関数として生成される要素ｅが、イデアルＱを法として$\phi_1 h_1 + \phi_2 h_2 +, \ldots, + \phi_k h_k + \phi_k + m$と合同であるＣ$_Q$の要素として生成されることを特徴とする請求の範囲第３２項に記載の方法。

３９．ｅ，ｆ$_1$，...，ｆ$_n$の関数Ｆを評価する結果Ａが積ｅ ｆ$_{k+1}$であることを特徴とする請求の範囲第３２項に記載の方法。

４０．ａ，ｆ$_1$，...，ｆ$_n$の関数Ｇを評価する結果Ｂが要素ａであることを特徴とする請求の範囲第３２項に記載の方法。

４１．ａ，ｆ$_1$，...，ｆ$_n$の関数Ｈを評価する代表剰余系のＣ$_P$集合中の結果ｃが、

ｃ ｆｋ＋１がイデアルＰを法としてｂと合同であるという条件を満たすことを特徴とする請求の範囲第３２項に記載の方法。

４２．結果ｃが、代表剰余系Ｃｐの集合中のメッセージｍの代表剰余系に等しいことを特徴とする請求の範囲第３２項に記載の方法。

４３．環Ｒが、次数Ｎのモニック多項式Ｍ（Ｘ）によって生成されるＲのイデアルを法として１つの変数Ｘ中の多項式の環であり、Ｒのイデアルｑが整数ｑによって生成されるイデアルであり、Ｒのイデアルｐが整数ｐによって生成されるイデアルであり、代表剰余系Ｃ０の集合が、次数がせいぜいＮ－１でｑを法とする代表剰余系の固定した集合中の係数を有するＲ中の多項式の集合であり、代表剰余系Ｃｐの集合が、次数がせいぜいＮ－１でｐを法とする代表剰余系の固定した集合中の係数を有するＲ中の多項式の集合であることを特徴とする請求の範囲第３２項に記載の方法。

４４．専用鍵要素ｆ１，．．．，ｆｎ、Ｒ中の専用メッセージ要素ｍ、および専用ランダム要素φ１，．．．，φｌが、その係数に対する境界を含むという条件を満たすことを特徴とする請求の範囲第４３項に記載の方法。

４５．環Ｒが非可換体であることを特徴とする請求の範囲第３２項に記載の方法。

４６．要素ｈ１，．．．，ｈｋが、１とＫの間の各ｉについて要素ｆｋ＋１ｈｉｆｋ＋２がイデアルＱを法としてＲ中でｆｉと合同であるという条件に従ってＣ０中で生成されることを特徴とする請求の範囲第３２項に記載の方法。

４７．専用鍵要素ｆ１，．．．，ｆｋがイデアルＰ中にあることを特徴とする請求の範囲第３２項に記載の方法。

４８．専用ランダム要素φ１，．．．，φ２ｋ＋１が、要素φ１，．．．，φｋがイデアルＰ中にあるという条件を満たすことを特徴とする請求の範囲第３２項に記載の方法。

４９．公開鍵要素ｈ１，．．．，ｈｋと、専用ランダム要素φ１，．．．，φ２ｋ＋１と、専用メッセージ要素ｍとの関数として生成される要素ｅが、イデアルＱを法としてφ１ｈ１φｋ＋１＋φ２ｈ２φｋ＋２＋，．．．，＋φｋｈｋφ２ｋ＋φ２ｋ＋１＋ｍと合同であるＣ０の要

素として生成されることを特徴とする請求の範囲第４５項に記載の方法。

５０．環Ｒが整数係数をもつ行列の環であり、Ｒのイデアルｑが、固定整数ｑで割り切れるすべての行列からなるイデアルであり、Ｒのイデアルｐが、固定整数ｐで割り切れるすべての行列からなるイデアルであり、代表剰余系C_qの集合が、ｑを法とする代表剰余系の固定した集合中の係数を有するＲの要素の集合であり、代表剰余系C_pの集合が、ｐを法とする代表剰余系の固定した集合中の係数を有するＲの要素の集合であることを特徴とする請求の範囲第３２項に記載の方法。

５１．専用鍵要素$f_1,\ldots,f_n$、専用メッセージ要素ｍ、および専用ランダム要素$\phi_1,\ldots,\phi_1$が、その係数に対する境界を含むという条件を満たすことを特徴とする請求の範囲第５０項に記載の方法。

５２．専用ランダム要素$\phi_1,\ldots,\phi_1$が、要素$\phi_1,\ldots,\phi_1$が単位行列の定数倍であるという条件を満たすことを特徴とする請求の範囲第５０項に記載の方法。

５３．環Ｒが群Ｇの群環であり、Ｒのイデアルｑが、整数ｑによって生成されるイデアルであり、Ｒのイデアルｐが、整数ｐによって生成されるイデアルであり、代表剰余系C_qの集合が、ｑを法とする代表剰余系の固定した集合中の係数を有するＲの要素の集合であり、代表剰余系C_pの集合が、ｐを法とする代表剰余系の固定した集合中の係数を有するＲの要素の集合であることを特徴とする請求の範囲第３２項に記載の方法。

５４．専用鍵要素$f_1,\ldots,f_n$、専用メッセージ要素ｍ、および専用ランダム要素$\phi_1,\ldots,\phi_1$が、その係数に対する境界を含むという条件を満たすことを特徴とする請求の範囲第５３項に記載の方法。

５５．環Ｒが、二面関係$X^N=1$、$Y^2=1$、$XY=YX^{N-1}$に従うことを条件として２つの変数ＸおよびＹ中の多項式の非可換環であり、Ｒのイデアルｑが整数ｑによって生成されるイデアルであり、Ｒのイデアルｐが整数ｐによって生成されるイデアルであり、代表剰余系C_qの集合が、次数がせいぜいＮ－１でｑを法とする代表剰余系の集合から選ばれた係数を有する変数ＸにおけるＲ中の多項式の集合であり、代表剰余系C_pの集合が、次数がせいぜいＮ－１でｐを法とする

代表剰余系の固定した集合から選ばれた係数を有する変数Ｘにおける Ｒ中の多項式の集合であることを特徴とする請求の範囲第３２項に記載の方法。

５６．専用鍵要素 $f_1,\ldots,f_n$、専用メッセージ要素ｍ、および専用ランダム要素 $\phi_1,\ldots,\phi_l$ が、その一部が、条件Ｙ $\phi=\phi$ Ｙを満たすＲのすべての要素 ϕ からなるＲの可換部分環 R_0 中にあるという条件を含む諸条件を満たすことを特徴とする請求の範囲第５５項に記載の方法。

【発明の詳細な説明】

公開鍵暗号システム方法および装置

関連出願

本出願は、１９９６年８月１９日に出願された米国仮特許出願第６０／０２４１３３号の優先権を主張するものであり、この仮特許出願は引用によって本明細書に組み込まれる。

発明の分野

本発明は、情報の符号化および復号に関し、詳細には、プロセッサ・システムによってデジタル・メッセージを暗号化し復号する公開鍵暗号システムに関する。

発明の背景

２つの当事者、たとえば、２つのコンピュータの間でデータを安全に交換するには暗号化が必要である。現在使用されている一般的な暗号化方法には、専用鍵暗号化と公開鍵暗号化の２つがある。専用鍵暗号化では、２つの当事者が符号化および復号に使用される鍵を秘密裏に交換する。専用鍵暗号システムの広く使用されている例にはＤＥＳ、すなわちデータ暗号化標準がある。このようなシステムは非常に高速であり、かつ非常に安全であるが、２つの当事者が鍵を秘密裏に交換しなければならないという欠点を有する。

公開鍵暗号システムは、各当事者が復号プロセスのセキュリティを損なわずに暗号化プロセスを公開することのできるシステムである。この暗号化プロセスは一般に落とし戸関数と呼ばれている。公開鍵暗号システムは、一般に専用鍵暗号システムよりも低速であるが、クレジット・カード番号など少量のデータを送信するために使

用され、また、専用鍵暗号化に使用される専用鍵を送信するためにも使用される。

従来、公開鍵暗号システムには様々な落とし戸関数が提案され実施されている。

公開鍵暗号システムを作成するために使用されているある種類の落とし戸関数

では、ある群のべき乗が使用され、すなわち、ある群の要素が取り出され、群演算を使用してその要素のべき乗が反復的に求められる。最も頻繁に選択される群は、大きな素数ｐおよびｑのｐｑを法とする乗法群である。ただし、楕円曲線、アーベル多様体、場合によっては非可換行列群など他の群も提案されている。しかし、この種の落とし戸関数は、それぞれ１００桁程度の大きな素数を必要とし、鍵の作成が面倒であり、暗号化および復号に使用されるべき乗プロセスは多数の計算を必要とし、Ｎビットからなるメッセージを暗号化し復号するには百桁の数の多数の乗算とN^3個程度の演算を必要とする。

公開鍵暗号システムを作成するために使用されている第２の種類の落とし戸関数は、群中のどの数が平方であるか、すなわち通常は、大きな素数ｐおよびｑのｐｑを法とする乗法群を判定するのが困難であることに基づく。第１の種類の場合と同様に、鍵作成が面倒であり、符号化および復号に多数の計算が必要であり、Ｎビットからなるメッセージを符号化し復号するにはN^3個程度の演算が必要である。

第３の種類の落とし戸関数では、群中で離散対数問題が使用され、一般には、大きな素数ｐを法とする乗法群または楕円曲線が使用される。この場合も、素数ｐが少なくとも１５０桁を必要とし、ｐ－１が大きな素因数を必要とするので、鍵作成は面倒である。このよ

うなシステムはべき乗を使用し、したがってこの場合も、Ｎビットからなるメッセージを符号化し復号するにはN^3個程度の演算を必要とする。

公開鍵暗号システムを作成するために使用されている第４の種類の落とし戸関数は、ナップサック問題または部分集合和問題に基づく。このような関数は、部分群、通常は、加算される正の整数の部分群を使用する。この種の多くの公開鍵暗号システムは、格子整約技法を使用して破られており、したがって、もはや安全なシステムとはみなされていない。

公開鍵暗号システムを作成するために使用されている第５の種類の落とし戸関数は、誤り訂正符号、特にゴッパ符号に基づく。このような暗号システムは、有限体、一般には２つの要素を含む有限体上で線形代数を使用する。このような暗

号システムに対する線形代数アタックがあり、したがって、安全な暗号システムの鍵は４００００ビット程度の大きな矩形行列である。これは大部分の応用分野で大きすぎる。

公開鍵暗号システムを作成するために使用されている第６の種類の落とし戸関数は、大きな次元Ｎの大きな格子で極めて短い基本ベクトルを見つけることが困難であることに基づく。このようなシステムの鍵は、N^2ビット程度の長さを有し、これは多くの応用分野では大きすぎる。また、このような格子整約公開鍵暗号システムは非常に新しく、したがって、そのセキュリティは完全には分析されていない。

したがって、大部分のユーザは、比較的短く容易に作成される鍵を比較的高速の暗号化プロセスおよび復号プロセスと組み合わせる公開鍵暗号システムを有することが望ましいと考えている。

本発明の目的は、鍵が比較的短く、かつ容易に作成され、符号化プロセスおよび復号プロセスを高速に実行することのできる公開鍵暗号化システムを提供することである。本発明の目的は、比較的低いメモリ要件を有し、かつセキュリティ・レベル、鍵長、符号化・復号速度、メモリ要件、帯域幅をかなり柔軟に兼ね合わせることを可能にする様々なパラメータに依存する公開鍵暗号化システムを提供することである。

発明の概要

本発明は、鍵長が他の一般的な公開鍵暗号システムの鍵長に匹敵する鍵を、ベクトルの大きな集合からほぼ無作為に選択することを可能にし、適切な（たとえば、現状では＝2^{80}）セキュリティ・レベルを備え、最も一般に使用されている公開鍵暗号システム、すなわち前述のべき乗暗号システムよりも１桁ないし２桁程度高速の符号化プロセスおよび復号プロセスを提供する。

本発明の公開鍵暗号システムの実施形態の符号化技法は、２つの数ｐおよびｑを法とする多項式代数および整約に基づく混合システムを使用し、それに対して復号技法は、妥当性が基本確率理論に依存する非混合システムを使用する。本発明の公開鍵暗号システムのセキュリティは、多項式混合システムとｐおよびｑを

法とする規約化の独立性との相互作用によってもたらされる。セキュリティは、実験によって観測されるように、たいていの格子では、最も短いベクトルよりもわずかに長いに過ぎない多数のベクトルがある場合に最も短いベクトルを見つけることが非常に困難であることにも依存する。

本発明の実施形態は、環Ｒのイデアルｐおよびｑを選択するステップと、環Ｒの要素ｆおよびｇを生成するステップと、要素F_q、

すなわちｆ（ｍｏｄ　ｑ）の逆数を生成し、F_p、すなわちｆ（ｍｏｄ　ｐ）の逆数を生成するステップと、ｇおよびF_qを使用して得ることのできる積とｍｏｄ　ｑで合同であるｈを含む公開鍵を生成するステップと、ｆおよびF_pを得ることのできる専用鍵を生成するステップと、公開鍵およびランダム要素φを使用してメッセージｍを符号化することによって符号化メッセージｅを生成するステップと、専用鍵を使用して符号化メッセージｅを復号することによって復号メッセージを生成するステップとを含む、デジタル・メッセージｍを符号化し復号する方法の形態である。

本発明の他の特徴および利点は、以下の詳細な説明と添付の図面から容易に明らかになろう。

図面の簡単な説明

図１は、本発明の実施形態を実施する際に使用することのできるシステムのブロック図である。

図２は、この流れ図で引用された補助流れ図と共に、本発明の実施形態を実施する際に使用することのできる公開鍵暗号化システムの流れ図である。

図３は、公開鍵および専用鍵を生成するための、本発明の実施形態によるルーチンの流れ図である。

図４は、公開鍵を使用してメッセージを符号化するための、本発明の実施形態による流れ図である。

図５は、専用鍵を使用して符号化メッセージを復号するための、本発明の実施形態による流れ図である。

図６は、公開鍵および専用鍵を生成する、本発明の他の実施形態によるルーチ

ンの流れ図である。

図７は、公開鍵を使用してメッセージを符号化するための、本発明の他の実施形態による流れ図である。

図８は、専用鍵を使用して符号化メッセージを復号するための、本発明の他の実施形態による流れ図である。

詳細な説明

図１は、本発明の実施形態を実施する際に使用できるシステムのブロック図である。２つのプロセッサ・ベース・サブシステム１０５および１５５は、セキュリティの保障されないチャネル５０、たとえば電話やインターネット通信チャネルなどの有線通信チャネルまたは無線通信チャネルを介して通信するように示されている。サブシステム１０５はプロセッサ１１０を含み、サブシステム１５５はプロセッサ１６０を含む。プロセッサ１１０および１６０とそれに関連する回路を後述のようにプログラムすると、これらを使用して本発明の実施形態を実装し、本発明の方法の実施形態を実現することができる。プロセッサ１１０および１６０はそれぞれ、任意の適切なプロセッサ、たとえば電子デジタル・プロセッサまたはマイクロプロセッサでよい。任意の汎用プロセッサまたは特殊目的プロセッサ、あるいは本明細書に記載した機能を電子的または光学的に、あるいは他の手段によって実行することのできる他の機械または回路を使用できることが理解されよう。プロセッサはたとえば、Ｉｎｔｅｌ　Ｐｅｎｔｉｕｍプロセッサでよい。サブシステム１０５は通常、メモリ１２３、クロック・タイミング回路１２１、入出力機能１１８、モニタ１２５を含み、これらはすべて従来型の種類のものでよい。入力には、１０３で示したキーボード入力を含めることができる。通信はトランシーバ１３５を介して行われ、トランシーバ１３５は、モデム、または信号を伝達する任意の適切な装置を備えることができる。

この例示的な実施形態のサブシステム１５５は、サブシステム１０５と同様な構成を有することができる。プロセッサ１６０は、関連する入出力回路１６４、メモリ１６８、クロック・タイミング回路１７３、モニタ１７６を有する。入力

にはキーボード１５５が含まれる。サブシステム１５５と外部との通信はトランシーバ１６２を介して行われ、この場合も、トランシーバ１６２はモデム、または信号を伝達する任意の適切な装置を備えることができる。

本発明の公開鍵暗号システム実施形態の符号化技法は、２つの数ｐおよびｑを法とする多項式代数および整約に基づく混合システムを使用し、それに対して復号技法は、妥当性が基本確率理論に依存する非混合システムを使用する。［多項式が順序係数の好都合な表現（いくつかの係数がゼロであってよい、Ｎ個の順序係数を有するＮ－１次の多項式）であり、プロセッサが、指定された演算を係数に対して実行することが理解されよう。］本発明の公開鍵暗号システムのセキュリティは、多項式混合システムとｐおよびｑを法とする規約化の独立性との相互作用によってもたらされる。セキュリティは、実験によって観測されるように、たいていの格子では、最も短いベクトルよりもわずかに長いに過ぎない多数のベクトルがある場合に最も短いベクトルを見つけることが非常に困難であることにも依存する。

本発明の暗号システムは、M. Blum他著「An Efficient Probabilistic Public-Key Encryption Scheme Which Hides All Partial Information」(Advanccs in Cryptology:Proccedings of CRYPTO 84,Lecture Notes in Computer Science、第１９６巻、Springer-Verlag、１９８５年、２８９ページないし２９９ページ)およびs. Goldwasser他著「Probabilistic Encryption」J.Computer and System s

Science 28(１９８４年)、２７０ページないし２９９ページ）に記載された確率暗号システムの一般的な枠組みに適合する。このことは、暗号化がランダム要素を含み、したがって各メッセージが多数の可能な暗号化を有することを意味する。符号化および復号ならびに鍵作成は、本発明の技法を使用して比較的高速にかつ容易に行われ、長さＮのメッセージ・ブロックを符号化または復号するのに必要な演算はＯ（N^2）個であり、したがって、ＲＳＡで必要とされるＯ（N^3）個の演算よりもかなり高速である。鍵長はＯ（Ｎ）であり、R.J.McEliece著「A Public-Key Cryptosystem Based On Algebraic Coding Thcory」(JPL Pasadena,DS

N Progress Reports 42-44(１９７８年)、１１４ページないし１１６ページ)および O. Goldreich等著「Public-Key Cryptosystems From Lattice Reduction Problems」(MIT-Laboratory for Computer Science再版、１９９６年１１月)に記載されたような他の「高速」公開鍵システムで必要とされるO（N^2）鍵長に匹敵する。

本発明の暗号システムの実施形態は、４つの整数パラメータ（N、K、p、q）と、整数係数を有するN－１次多項式の３つの集合L_q、L_ϕ、L_mとに依存する。この実施形態は、環R＝Z［X］／（X^N-1）で働く。要素F∈Rは多項式またはベクトルとして書かれる。

$$F = \sum_{i=1}^{N} F_i X^{N-i} = [F_1, F_2, ..., F_N]$$

星印「*」はRの乗算を示す。この星印乗算は巡回畳み込み積、すなわち次式のF*G＝Hとして明示的に与えられる。

$$H_k = \sum_{i=1}^{k-1} F_i G_{k-i} + \sum_{j=1}^{N} F_i G_{N+k-i} = \sum_{i+j=k(\mathrm{mod}N)} F_i G_j$$

（たとえば）qを法とする乗算を実行する際、係数はqを法として整約される。詳細は、付録１を参照されたい。

以下に公開鍵暗号システムの発明による実施形態の例を示す。例示を容易にするために非常に小さな数が使用されており、したがって、この例は暗号に関して安全ではない。例と共に、二重括弧（[[ ]]）内のマテリアルとして、現在の条件の下で暗号に関して安全な実際的な暗号システムを形成する動作パラメータについて説明する。特定のセキュリティ・レベルを達成する動作パラメータの詳細な議論は付録１に記載されている。付録１には、本発明の暗号システムの実施形態の、様々なアタック・タイプに対する耐性についても記載されている。

本発明の実施形態で使用される対象はN－１次の多項式である。

$$a_1 x^{N-1} + a_2 x^{N-2} + ... + a_{N-1} x + a_N$$

上式で、係数$a_1, ..., a_N$は整数である。本発明の「星印」乗算では、x^Nが１で置き換えられ、x^{N+1}がXで置き換えられ、x^{N-2}がx^2で置き換えられ、以下同様である。［多項式をN組の数

［ａ１，ａ２，．．．，ａＮ］

で表すこともできる。このような場合、星印積を畳み込み積とも呼ぶ。Ｎの値が大きい場合、実行するステップがＮ^{2}個ではなくＮｌｏｇＮ個程度である高速フーリエ変換法を使用して畳み込み積をより高速に計算することができる。］たとえば、Ｎ＝５とし、２つの例示的な多項式を用いた場合、星印乗算は以下の数式を与える。

$(x^4+2x^2-3x+2)*(2x^4+3x^3+5x-1)$

$=2x^8+3x^7+4x^6+5x^5-6x^4+16x^3-17x^2+13x-2$

$=2x^3+3x^2+4x+5x-6x^4+16x^3-17x^2+13x-2$

$=-6x^4+18x^3-14x^2+17x+3$

［［安全なシステムはたとえば、Ｎ＝１６７またはＮ＝２６３を使用することができる］］［この実施形態は、ｘ^N－１のすべての倍数からなるイデアルを法とする整数係数を含む多項式の環を使用する。より一般的には、異なるイデアルを法とする多項式を使用することができる。さらに一般的には、他の何らかの環Ｒを使用することができる。環およびイデアルの詳細については、たとえば、I.N.Herstein著「Topics in Algebra」を参照することができる。

この実施形態の他の態様では、イデアルｑなどの整数を法として多項式の係数が整約される。このことは基本的に、各係数をｑで除し、係数をその剰余で置き換えることを意味する。たとえば、ｑ＝１２８であり、ある係数が２３７７である場合、２３７７を１２８で除すると１８であり、剰余が７３であるので、この係数は７３で置き換えられる。しかし、「対称剰余」を使用した方が容易である。このことは、剰余が０ないしｑ／２である場合、係数はそのままであるが、ｑ／２ないしｑである場合は係数からｑが減じられることを意味する。したがって、ｑ＝１２８に対称剰余を使用する場合、－５５＝７３－１２８であるので２３７７は－５５で置き換えられる。

この剰余プロセスが実行されていることを示すには、３重等号（≡）を符号「ｍｏｄ　ｑ」と共に使用する。以下に、２つの多項式の星印乗算を５を法とする規約化と組み合わせる例を示す。答えには対称剰余が使用される。

$(x^4+2x^2-3x+2)*(2x^4+3x^3+5x-1)=-6x^4+18x^3-14x^2+17x+3$

$\equiv -x^4-2x^3+x^2+2x-2 \pmod 5$

本発明の実施形態によって（かつ例示を容易にするために、上記で指摘した小さな数を用いて）公開鍵暗号システムを作成する際、

第１のステップは整数パラメータＮ、Ｋ、ｐ、ｑを選択することである。以下に例を示す。

Ｎ＝５、Ｋ＝１、ｐ＝３、ｑ＝１２８

[[安全なシステムはたとえば、Ｎ＝１６７、Ｋ＝６、ｐ＝３、ｑ＝2^{16}＝６５５３６を使用することができる]] 好ましくは、ｐとｑは互いに素であり、すなわち、１よりも大きな共通因子を有さない。イデアルｐとイデアルｑを互いに素にすることが望ましいことについては付録１に記載されている。以下のように、多項式のいくつかの集合が選択される。

L_g＝｛係数が－２、－１、０、１、２である多項式｝

L_ϕ＝｛２つの－１、２つの１、１つの０を係数として有する多項式｝

L_m＝｛係数が－１、０、１である多項式｝

[[安全なシステムはたとえば、以下の集合を使用することができる。

L_g＝｛係数が－１７７ないし１７７である多項式｝

L_ϕ＝｛係数が４０個の１、４０個の－１、残りの０である多項式｝

L_m＝｛係数が－３ないし３である多項式｝

（注：多項式はＮ－１次を有し、したがって、この例の安全なパラメータの場合、多項式は１６６次を有する。さらに、符号化されている実際のメッセージｍの係数をｐ、すなわちこの例ではｐ＝３で除すると、このメッセージは剰余で構成される）]]。

集合L_gは、暗号システムの鍵を作成するために使用され、集合L_ϕはメッセージを符号化するために使用され、集合L_mは、可能なメッセージの集合である。たとえば、

$2x^4-x^3+x-2$は集合L_gに存在し、

$x^4-x^3-x^2+1$は集合L_ϕに存在する。

鍵作成者Ｄａｎは、この例の鍵作成を実施するとき、集合L_gから２つの多項式ｆおよびｇを選択する。この簡略化された例ではＫ＝１であり、したがって１つの多項式ｇのみが存在する。Ｄａｎが次式を選択するものと仮定する。

$$f=x^4-x^3+2x^2-2x+1$$

$$g=x^4-x^3+x^2-2x+2$$

[[安全なシステムはたとえば、Ｋ＋１個の多項式ｆ，$g_1,\ldots,g_K\in L_g$をＫ＝６と共に使用することができる。]]

本発明の要件は、ｆが、ｑを法とする逆数とｐを法とする逆数を有さなければならないことである。このことは、次式が成立するように多項式F_qおよびF_pが存在しなければならないことを意味する。

$$F_q*f\equiv 1 \pmod q \text{ および } F_p*f\equiv 1 \pmod p$$

周知のユークリッド・アルゴリズムを使用してF_qおよびF_pを算出することができる。たとえば、本明細書の付録ＩＩを参照することができる。（いくつかのｆが逆数を有さないことがある。この場合、Ｄａｎは最初に戻り、別のｆを選択する。）上記の例ｆでは、次式が成立する。

$$F_q=103x^4+29x^3+116x^2+79x+58$$

$$F_p=2x^4+2x$$

これがｆの正しいF_qであることを検査するには、以下の乗算を行うことができる。

$$F_q*f=(103x^4+29x^3+116x^2+79x+58)*(x^4-x^3+2x^2-2x+1)$$

$$=256x^4+256x-127$$

$$\equiv 1 \pmod{128}$$

同様に、F_pが正しいことを検査するには、以下の乗算を行うことができる。

$$F_p*f=(2x^4+2x)*(x^4-x^3+2x^2-2x+1)$$

$$=6x^3-6x^2+6x-2$$

$$\equiv 1 \pmod 3$$

これで、鍵作成者Ｄａｎが自分の公開鍵、すなわち、次式によって与えられる

多項式ｈを作成する準備が完了した。

$$h \equiv F_q * g \pmod q$$

[[安全なシステムは、次式によって与えられるＫ個の多項式$h_1, \ldots, h_K$を使用することができる。]]

$$h_i \equiv F_q * g_i \pmod q、\ i=1,2,\ldots,K、\ K=6$$

この例では続いて、Ｄａｎが次式を計算する。

$$F_q * g = (103x^4+29x^3+116x^2+79x+58) * (x^4-x^3+x^2-2x+2)$$

$$=243x^4-50x^3+58x^2+232x-98$$

$$\equiv -13x^4-50x^3+58x^2-24x+30 \pmod{128}$$

Ｄａｎの公開鍵は以下の多項式である。

$$h=-13x^4-50x^3+58x^2-24x+30$$

Ｄａｎの専用鍵は多項式対（ｆ，F_p）である。原則的に、F_pは常にｆから計算することができるので、多項式ｆ自体が専用鍵として働くことができる。しかし、実際には、Ｄａｎはおそらく、F_pを事前に算出し保存しておく必要がある。

この例の次の部分における専用鍵による符号化について説明する。符号化側Ｃａｔｈｙが Ｄａｎの公開鍵ｈを使用してＤａｎにメッセージを送信する必要があると仮定する。Ｃａｔｈｙは可能なメッセージの集合L_mからあるメッセージを選ぶ。たとえば、Ｃａｔｈｙが以下のメッセージを送信すると仮定する。

$$m=x^4-x^3+x^2+1$$

Ｃａｔｈｙは、このメッセージを符号化するとき、集合L_ϕから無作為に多項式ϕを選択する。たとえば、Ｃａｔｈｙは次式を選択する。

$$\phi=-x^4+x^3-x^2+1$$

Ｃａｔｈｙは、無作為に選択したこの多項式ϕ、Ｄａｎの公開鍵ｈ（ならびにｐおよびｑ、すなわち、公開鍵の一部）、Ｃａｔｈｙの平文メッセージを使用し、以下の公式を使用して符号化メッセージｅを作成する。

$$e \equiv p\phi * h + m \pmod q$$

[[安全なシステムはＫ個の公開鍵$h_1, \ldots, h_K$を、安全な例についてのＫ＝６と

共に使用することができる。Ｃａｔｈｙは、メッセージを符号化するときに、集合L_ϕからＫ個の多項式$\phi_1,\ldots,\phi_K$を無作為に選択し、次いで$e\equiv p\phi_1*h_1+p\phi_2*h_2+\ldots+p\phi_K*h_K+m \pmod q$を計算することによって符号化メッセージｅを作成することができる。]] 別法として、ｈが$pF_q*g \pmod q$と等しくされ、その場合、公式$e\equiv\phi*h+m \pmod q$を使用してメッセージを符号化することができる。この例では、Ｃａｔｈｙは以下の計算を行う。

$$p\phi*h+m=3(-x^4+x^3-x^2+1)*(-13x^4-50x^3+58x^2-24x+30)+(x^4-x^3+x^2+1)$$

$$=-374x^4+50x^3+196x^2-357x+487$$

$$\equiv 10x^4+50x^3-60x^2+27x-25 \pmod{128}$$

したがって、Ｃａｔｈｙの符号化メッセージは以下の多項式であり、

$$e=10x^4+50x^3-60x^2+27x-25$$

Ｃａｔｈｙはこの符号化メッセージをＤａｎに送信する。

この例の次の部分における専用鍵を使用した復号について説明する。Ｄａｎは、メッセージｅを復号するためにまず、専用鍵ｆを使用して以下の多項式を計算する。

$$a\equiv f*e \pmod q$$

使用中の例では、Ｄａｎは以下の計算を行う。

$$f*e=(x^4-x^3+2x^2-2x+1)*(10x^4+50x^3-60x^2+27x-25)$$

$$=-262x^4+259x^3-124x^2-13x+142$$

$$\equiv -6x^4+3x^3+4x^2-13x+14 \pmod{128}$$

したがって、多項式ａは次式で表される。

$$a=-6x^4+3x^3+4x^2-13x+14$$

次に、ＤａｎはＦｐ、すなわち自分の専用鍵の他方の半分を使用して以下の計算を行う。

$$F_p*a \pmod p$$

この結果が復号メッセージである。したがって、この例では、Ｄａｎは以下の計算を行う。

$$F_p * a = (2x^4+2x) * (-6x^4+3x^3+4x^2-13x+14)$$
$$= 34x^4-4x^3-20x^2+36x-38$$
$$\equiv x^4-x^3+x^2+1 \pmod 3$$

この復号がなぜ有効であるかの詳細な説明については、付録Ｉを参照することができる。

本発明の他の実施形態では、環は行列の環である。たとえば、環　Ｒ＝（整数係数を有するＭ×Ｍ個の行列の環）を使用することができる。

Ｒの要素を以下に示す。

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1M} \\ a_{21} & a_{22} & & a_{2M} \\ \vdots & & \ddots & \vdots \\ a_{M1} & a_{M2} & \cdots & a_{MM} \end{pmatrix}$$

上式で係数ａｉｊは整数である。加算および乗算は、行列に対して通常行われる加算および乗算であり、このプロセッサが行列のメンバーを、従来型の方式で記憶され処理される数として扱えることが理解されよう。Ｎ＝Ｍ^{2}である場合、Ｒの行列はＮ個の係数を有する。互いに素な整数ｐとｑが選択される。

この場合、Ｄａｎは、専用鍵を作成するために、ＲからＫ＋２個の行列を選択する。これらの行列を

$$f, \quad g, \quad w_1, \quad w_2, \ldots, w_K$$

と呼ぶ。これらの行列は、ｆ，　ｇ，$w_1, \ldots, w_K$がかなり小さな係数を有し、あらゆるw_iが次式を満たすという特性を有するべきである。

$$w_i \equiv 0 \quad (\mathrm{mod} \quad p)$$

（言い換えれば、あらゆるw_iのあらゆる係数がｐの倍数である。）Ｄａｎは、自分の鍵を作成するときに、ｐおよびｑを法とするｆおよびｇの逆数を見つける必要がある。したがって、Ｄａｎは、次式を満たすＲ内の行列F_p、F_q、G_p、G_qを見つける。

$$f F_p \equiv I \quad (\mathrm{mod} \quad p)$$
$$f F_q \equiv I \quad (\mathrm{mod} \quad q)$$

$$g G_p \equiv I \pmod{p}$$

$$g G_q \equiv I \pmod{q}$$

上式で、ＩはＭ×Ｍ識別行列である。一般に、これを実行するのは容易であり、何らかの理由で１つの逆数が存在しない場合でも、Ｄａｎは新しいｆまたはｇを選択するだけでよい。

Ｄａｎの公開鍵は、以下の条件によって決定されるＫ個の行列（h_1，h_2，...，h_K）の並びである。

$$h_i \equiv F_q w_i G_q \pmod{q} \quad (i = 1, 2, \ldots, K)$$

（w_iがｐを法とするゼロと合同であることに留意されたい。）Ｄａｎの専用鍵は４つの行列（ｆ，ｇ，F_p，G_p）である。原則的に、ｆおよびｇのみを専用鍵として使用できるが、実際にはF_p、G_pを事前に計算し記憶しておいた方が効率的である。

この行列の例の符号化について次に説明する。Ｃａｔｈｙがメッセージｍを符号化する必要があるものと仮定する。メッセージｍは、ｐを法とする係数を有する行列である。Ｃａｔｈｙは、自分のメッセージを符号化するために、ある条件を満たすいくつかの整数$\phi_1, \ldots, \phi_K$を無作為に選択する。たとえば、これらの整数としては、和$\phi_i + \ldots + \phi_K$が所定の値ｄと等しい非負整数を選択することができる。（ϕ_iが通常の整数であり、行列ではないことに留意されたい。同様に、ϕ_iは、識別行列の倍数とみなすことができ、したがって環Ｒのあらゆる要素と交換することができる。）

Ｃａｔｈｙは、自分のϕ_iを選択した後、以下の規則によって符号化メッセージｅを作成する。

$$e \equiv \phi_1 h_1 + \phi_2 h_2 + \ldots + \phi_K h_K + m \pmod{q}$$

次に、この行列の例の復号について説明する。Ｄａｎが符号化メッセージｅを受信しており、それを解読する必要があるものと仮定する。Ｄａｎはまず、次式を満たす行列ａを計算する。

$$a \equiv f e g \pmod{q}$$

Ｄａｎは、通常どおり、－ｑ／２ないしｑ／２（すなわち、ゼロ対称係数）や０

ないしｑ－１など、ある限られた範囲内でａの係数を選択する。

パラメータが適切に選択される場合、行列ａは以下の和に丁度等しくなる。

$$a = \phi_1 w_1 + \phi_2 w_2 + \ldots \phi_K w_K + fmg$$

（これは常に、ｑを法として真であるが、重要な点は、ｑが十分大きい場合に、上式が、ｑを法とする場合だけではなく厳密な等式になることである。）Ｄａｎの次のステップは、たとえば次式のように、ｐを法としてａを整約することである。

$$b \equiv a \pmod{p}$$

w_iのすべての係数をｐで除することができるので、これは、以下のことを意味する。

$$b \equiv fmg \pmod{p}$$

最後に、Ｄａｎは以下の計算を行い、

$$F_p b G_p \pmod{p}$$

最初のメッセージｍを再生する。

前述のＭ×Ｍ行列の実施形態は優れた動作時間を有する。符号化は、加算しか必要とせず、M^2個程度の演算を実行する。復号はＭ×Ｍ行列の２回の行列乗算を必要とし、したがって、M^3個の演算を実行する。メッセージ長はM^2程度であり、したがって、Ｎが固有メッセージ長（すなわち、$N=M^2$）を示す場合、行列実施形態は、符号化にはＯ（Ｎ）個のステップを必要とし、復号にはＯ（$N^{3/2}$）個のステップを必要とする。これに対して、多項式実施形態は、符号化にＯ（N^2）個のステップを必要とし、復号にＯ（N^2）個のステップを必要とし、ＲＳＡ公開鍵システムは、符号化にＯ（N^3）個のステップを必要とし復号にＯ（N^3）個のステップを必要とする。

予備的な分析により、次元がN^2+N（またはそれ以上）である

格子を使用する必要があるのは、行列実施形態に対する固有格子アタックだけであることがわかっている。これは、多項式実施形態を解読するために使用される２Ｎ次元格子に対する著しいセキュリティの向上である。

暴力的（または潜在的なｍｅｅｔ－ｉｎ－ｔｈｅ－ｍｉｄｄｌｅ）アタックを回避するには、ϕ_iのサンプル空間をかなり大きくし、たとえば2^{100}ないし2^{200}にする必要がある。しかし、こうするのは困難である。たとえば、ϕ_iが、和ｄを有する非負の値として選択された場合、サンプル空間は、

$$\binom{d+K-1}{K-1}=\frac{(d+K-1)!}{d!(K-1)!}$$

個の要素を有する。したがって、たとえばＫ＝１５およびｄ＝１０２４を選択した場合、$2^{103.8}$個の要素を有するサンプル空間が得られる。

公開鍵サイズは$KM^2 \log_2(g)$ビットであり、専用鍵サイズは$2M^2 \log_2(pq)$ビットである。これらは共に実際的なサイズである。

図２は、公開鍵暗号化システムと共に使用できる基本手順を示し、本発明の実施形態による特徴を説明する参照される他の流れ図によって示されるルーチンを指す。ブロック２１０は、公開鍵情報および専用鍵情報の生成と、公開鍵の「公開」を表す。本発明の実施形態のルーチンについて図３の流れ図に関して説明する。この例では、この演算がプロセッサ・システム１０５で実行されるものと仮定することができる。公開鍵情報は、公開することができ、すなわち、公衆の任意のメンバー、または専用鍵保持者が暗号化メッセージを受信する必要のある所望の群に利用させることができる。通常、

必ずしも必要ではないが、公開鍵保持者およびその公開鍵のディレクトリが維持されている中央公開鍵ライブラリ施設またはウェブサイトで公開鍵を利用可能にすることができる。この例では、プロセッサ・システム１５５のユーザがプロセッサ・システム１０５のユーザに秘密のメッセージを送信する必要があり、プロセッサ・システム１５５のユーザがプロセッサ・システム１５０のユーザの公開済みの公開鍵を知っているものと仮定する。

ブロック２２０は、所期のメッセージ受信側の公開鍵を使用して平文メッセージを符号化するためにメッセージ送信側（すなわち、この例ではプロセッサ・システム１５５のユーザ）によって使用することのできるルーチンを表す。本発明の実施形態によるこのルーチンについては、図４の流れ図に関して説明する。こ

の場合、暗号化メッセージはチャネル５０（図１）を介して送信される。

図２のブロック２６０は、暗号化メッセージを復号して平文メッセージを再生するルーチンを表す。この例では、この機能は、専用鍵情報を使用するプロセッサ・システム１０５のユーザによって実行される。本発明の実施形態の復号ルーチンについては図５の流れ図に関して説明する。

次に、図３を参照すると、全体的に図２のブロック２１０で表された、公開鍵および専用鍵を生成するルーチンの流れ図が示されている。このルーチンはこの例では、プロセッサ・システム１０５のプロセッサ１１０をプログラムするために使用することができる。ブロック３０５は、整数パラメータＮ、ｐ、ｑの選択を表す。前述のように、Ｎは、生成される多項式ｆおよびｇiの次数を決定し、ｐおよびｑはそれぞれ、星印積を生成する際に使用される２つのイデアルである。ブロック３１５はＫ、すなわち使用される多項式ｇ

iの数を表す。上記の簡略化された例では、Ｋは１であり、例示的で比較的安全な特定のシステムがＫ＝６を使用できることに留意されたい。次に、ブロック３２５は無作為な多項式ｆ、g_1、$g_2 \ldots g_K$の選択を表す。係数はたとえば、乱数発生装置を使用して選択することができ、乱数発生装置は、利用可能なハードウェアまたはソフトウェアを使用して周知の方法で実装することができる。この実施形態では、各プロセッサ・システムが乱数発生装置を備え、乱数発生装置は図１ではそれぞれ、ブロック１３０および１８５で指定されている。

ブロック３４０は、選択済みの多項式ｆの逆数F_qおよびF_pが存在する場合に、それらの逆数を前述のように求めるためにユークリッド・アルゴリズムを応用することを表す。F_p、F_qが存在しない場合、再びブロック３２５に入り、新しい多項式ｆが選択される。ループ３３０は、定義済みの逆数を算出できる多項式が選択されるまで継続する。［所与の多項式について逆数が存在する確率は比較的高く、したがって一般に、この条件が満たされるまでにループ３３０を横断する回数は比較的少ないことが予期される。］次いで、ブロック３５０に入る。このブロックは前述のように、

$$h = F_q * g \pmod{q}$$

による公開鍵ｈの計算を表す。［Ｋ＞１の場合、ｉ＝１，２，．．．．Ｋについて公開鍵構成要素ｈｉがある。］ブロック３６０で表されるように、専用鍵は多項式ｆ、Ｆｐとして保持され、この場合、ブロック３７０で表されるように、公開鍵を公開することができる。

図４は、平文メッセージｍの符号化を実施するようにプロセッサ・システム１５５（図１）のプロセッサ１６０などのプロセッサをプログラムするルーチンの、図２のブロック２４０によって一般

的に表される流れ図である。符号化されるメッセージが入力され(ブロック４２０)、ランダム多項式φが選択される(ブロック４３０)。［Ｋ＞１の場合、Ｋ個の無作為多項式φ１，φ２，．．．．，φＫが選択される。］この多項式は、前述のように集合Ｌφの多項式でよく、ランダム係数は、任意のハードウェア手段またはソフトウェア手段、たとえば、乱数発生装置１８５によって選択することができる。次いで、符号化メッセージｅを次式のように算出することができる(ブロック４５０)。

$$e = p\phi * h + m \pmod{q}$$

上記で指摘したように、Ｋが１よりも大きい場合、符号化メッセージは$e \equiv p\phi_1 * h_1 + p\phi_2 * h_2 + \ldots + p\phi_K * h_K + m \pmod{q}$になる。この符号化メッセージは、チャネル５０を介して鍵保持者、すなわち、この例ではプロセッサ・システム１０５のユーザに送信する（ブロック４６０）ことができる。

図５は、図２で全体的にブロック２６０によって表された、暗号化メッセージを復号する本発明の実施形態によるルーチンの流れ図である。ブロック５３０は暗号化メッセージｅの受信を表す。定義済みの多項式ｆおよびＦｐと整数Ｎ、ｐ、ｑとを含む保持されている専用鍵情報が取り出される(ブロック５５０)。次に、ブロック５７０は次式の計算を表している。

$$a \equiv f * e \pmod{q}$$

次いで、本明細書ではｍ’として指定された復号メッセージを次式のように算出することができる(ブロック５８０)。

$$m' \equiv F_p * a \pmod{p}$$

図６、図７、図８は、前述の行列実施形態に関する流れ図である。図６は、全体的に図２のブロック２１０によって表された、公開鍵

および専用鍵を生成するルーチンの流れ図である。前述のように、このルーチンをこの例で使用して、プロセッサ・システム１０５のプロセッサ１１０をプログラムすることができる。ブロック６０５は、整数パラメータＮ、ｐ、ｑの選択を表し、Ｎは行列係数の数であり、ｐおよびｑは互いに素な整数である。ブロック６１５はＫの選択を表し、Ｋを選択することによって行列の数が決定される。次に、ブロック６２５はランダム行列ｆ，ｇ，w_1，w_2，...，w_Kの選択と、w_1，w_2，...，w_Kがすべて、ｐを法として０と合同であるという要件とを表す。この場合も、この目的のために乱数発生装置１３０（図１）を使用することができる。

ブロック６４０は、定義済みの行列F_p、F_q、G_p、G_qの決定を表す。これらの行列が存在しない場合、再びブロック６２５に入り、新しい行列ｆおよびｇが選択される。ループ６３０は、定義済みの逆数を算出できる行列が選択されるまで継続する。次いで、ブロック６５０に入る。このブロックは、公開鍵、すなわち、以下の条件によって決定されるＫ個の行列（h_1，h_2，...，h_K）のリストの算出を表す。

$$h_i \equiv F_q w_i G_q \pmod{q} \quad (i=1,2,\ldots,K)$$

ブロック６６０で表されているように、専用鍵は行列（ｆ，ｇ，F_p，G_p）として保持され、その場合、ブロック６７０で表したように公開鍵を公開することができる。

図７は、この行列実施形態の技法を使用して平文メッセージｍの符号化を実施するようにプロセッサ・システム１５５（図１）のプロセッサ１６０などのプロセッサをプログラムする、全体的に図２のブロック２４０で表されたルーチンの流れ図である。符号化されるメッセージが入力され(ブロック７２０)、ランダム整数ϕ_1，

ϕ_2，...，ϕ_Kが選択される(ブロック７３０)。これらの整数は乱数発生装置１８

５（図１）によって選択することができる。次いで、符号化メッセージｅを次式のように算出することができる(ブロック７５０)。

$$e \equiv \phi_1 h_1 + \phi_2 h_2 + \ldots + \phi_k h_k + m \pmod{q}$$

この符号化メッセージは、チャネル５０を介して鍵保持者、すなわち、この例ではプロセッサ・システム１０５のユーザに送信することができる(ブロック７６０)。

図８は、図２で全体的にブロック２６０によって表された、この行列実施形態によって暗号化メッセージを復号するルーチンの流れ図である。ブロック８３０は暗号化メッセージｅの受信を表す。定義済みの多項式Ｆ、ｇ、F_p、G_pと整数Ｎ、ｐ、ｑとを含む保持されている専用鍵情報が取り出される(ブロック８５０)。次に、ブロック８７０は次式の計算を表している。

$$a \equiv f e g \pmod{q}$$

次に、ａは、次式のように、ｐを法としてｂに整約される(ブロック８８０)。

$$b \equiv a \pmod{p}$$

次いで、次式のように復号メッセージが算出される(ブロック８９０)。

$$m' \equiv F_p b G_p \pmod{p}$$

特定の好ましい実施形態を参照して本発明を説明したが、当業者には本発明の趣旨および範囲内の変形形態が企図されよう。たとえば、公開鍵または専用鍵を任意の適切な媒体、たとえば「スマート・カード」上に記憶し、符号化および／または復号を実行できるマイクロプロセッサをこのスマート・カードに備え、それによって

暗号化メッセージをスマート・カードへ伝達し、かつ／あるいはスマート・カードから伝達することができることが理解されよう。

ＮＴＲＵ：環ベースの公開鍵暗号システム

JEFFREY HOFFSTEIN、JILL PIPHER、JOSEPH H. SILVERMAN

要約　ＮＴＲＵ、すなわち新規の公開鍵暗号システムについて説明する。ＮＴＲＵは、鍵がかなり短く容易に作成されること、高速であること、およびメモリ要

件が低いことを特徴とする。ＮＴＲＵの符号化および復号は、基本確率理論に基づくクラスタ化原則と組み合わされた、多項式代数によって提案されている混合システムを使用する。ＮＴＲＵ暗号システムのセキュリティは、多項式混合システムと、互いに素な２つの整数ｐおよびｑを法とする整約の独立性との相互作用によってもたらされる。

目次

§０．はじめに

ＤｉｆｆｅおよびＨｅｌｌｍａｎ［４］が、どのようにすれば１方向関数を使用して効率的で計算コストの低い公開鍵暗号を作成できるかについて説明して以来、このようなシステムの作成にかなりの関心が払われている。現在の所、最も広く使用されている公開鍵システムはＲＳＡである。ＲＳＡは、１９７８年にＲｉｖｅｓｔ、Ｓｈａｍｉｒ，Ａｄｅｌｍａｎによって作成されたものであり［１０］、大きな数を因数分解することが困難であることに基づく。他のシステムには、誤り補正符号に依存するＭｃＥｌｉｅｃｅシステム［９］と、格子整約問題の難点に基づくＧｏｌｄｒｅｉｃｈ、Ｇｏｌｄｗａｓｓｅｒ、Ｈａｌｅｖｉ［５］の最近のシステムが含まれる。

この論文では、新規の公開鍵暗号システムについて説明する。この暗号システムをＮＴＲＵシステムと呼ぶ。符号化手順では、多項式代数と２つの数ｐおよびｑを法とする整約に基づく混合システムを使用し、これに対して、復号手順では、妥当性が基本確率理論に依存する非混合システムを使用する。ＮＴＲＵ公開鍵

暗号システムのセキュリティは、多項式混合システムと、互いに素な２つの整数ｐおよびｑを法とする整約の独立性との相互作用によってもたらされる。セキュリティは、（実験によって観測されるように）、たいていの格子では、（適度に短いベクトルではなく）極めて短いベクトルを見つけることが困難であることにも依存する。

この論文で発表する内容は、すでに広く配布されているが未公表の前刷り［７］とは２つの主要な点で異なる。第１に、より良好な動作特性を有するシステムを生成するために使用できる新しいパラメータＫを導入した。第２に、主として、ｅメールを介してＤｏｎＣｏｐｐｅｒｓｍｉｔｈ、Ｊｏｈａｎ Ｈａｓｔａｄ、Ａｄｉ Ｓｈａｍｉｒから頂いた多数のコメントと最近の論文［３］中の多数のコメントに基づいて、格子ベースのアタックの分析を展開し明確

化した。この機会を利用して、この研究に関心を抱き援助していただいた上記の各氏に対して謝意を表したい。

ＮＴＲＵは、［１］および［６］に記載されたように確率暗号システムの一般的な枠組みに適合する。このことは、暗号化がランダム要素を含み、したがって各メッセージが多数の可能な暗号化を有することを意味する。ＮＴＲＵを用いた符号化および復号は極めて高速であり、鍵の作成は高速で容易である。詳細は第４章および第５章を参照されたいが、ＮＴＲＵでは、長さＮのメッセージ・ブロックを符号化または復号するのに必要な演算がＯ（N^2）個であり、ＲＳＡで必要とされるＯ（N^3）個の演算よりもかなり高速であることに留意されたい。さらに、ＮＴＲＵ鍵長はＯ（Ｎ）であり、［９，５］など他の「高速」公開鍵で必要とされるＯ（N^2）鍵長に匹敵する。

§１　ＮＴＲＵアルゴリズムの説明

§１．１　表記法

ＮＴＲＵ暗号システムは、４つの整数パラメータ（Ｎ、Ｋ、ｐ、ｑ）と、整数係数を有するＮ－１次多項式の３つの集合L_g、L_ϕ、L_mに依存する。環Ｒ＝Ｚ［Ｘ］／（X^N-1）を使用する。要素Ｆ∈Ｒを多項式またはベクトルとして書く。

$$F=\sum_{i=1}^{N}F_iX^{N-i}=[F_1,F_2,\ldots,F_N]$$

⊗を使用してＲの乗算を示す。この星印乗算は、巡回畳み込み積と

して明示的に与えられる。

$$H_k=\sum_{i=1}^{k-1}F_iG_{k-i}+\sum_{j=k}^{N}F_iG_{N+k-i}=\sum_{i+j=k(\mathrm{mod}\ N)}F_iG_j$$ の場合、Ｆ⊗Ｇ=Ｈ

（たとえば）ｑを法とする乗算を行う際、ｑを法として係数を整約

する。

注　原則的に、積Ｆ⊗Ｇの計算にはＮ２回の乗算が必要である。しかし、ＮＴＲＵによる典型的な積の場合、ＦとＧのうちの一方が小さな係数を有し、したがって、Ｆ⊗Ｇの計算は非常に高速である。一方、Ｎが大きいとみなされる場合は、高速フーリエ変換を使用してＯ（Ｎｌｏｇ Ｎ）個の演算で積Ｆ⊗Ｇを計算した方が高速である。

§１．２　鍵の作成

ＮＴＲＵ鍵を作成する場合、Ｄａｎは、Ｋ＋１個の多項式ｆ，$g_1,\ldots,g_K\in L_g$を無作為に選択する。多項式ｆは、ｑおよびｐを法とする逆数を有するという追加の要件を満たさなければならない。パラメータが適切に選択される場合、これはｆの大部分の選択肢について真であり、これらの逆数の実際の計算は、修正されたユークリッド・アルゴリズムを使用して容易に行うことができる。これらの逆数をF_qおよびF_pによって示す。

$$F_q\otimes f\equiv 1\ (\mathrm{mod}\ q)\quad および\quad F_p\otimes f\equiv 1\ (\mathrm{mod}\ p)\qquad (1)$$

Ｄａｎは次に、以下の数量を計算する。

$$h_i\equiv F_q\otimes g_i\ (\mathrm{mod}\ q)\quad 1\leq i\leq K\qquad (2)$$

Ｄａｎの公開鍵は、以下に示す多項式の並びである。

$$(h_1,\ h_2,\ldots,\ h_K)$$

Ｄａｎの専用鍵は単一の多項式ｆである。ただし、実際には、ＤａｎはＦｐを記憶する必要がある。

§１．３　符号化

Ｃａｔｈｙ（符号化側）がＤａｎ（復号側）にメッセージを送信する必要があるものと仮定する。Ｃａｔｈｙはまず、１組の平文Ｌｍからメッセージｍを選択する。次に、ＣａｔｈｙはＫ個の多項式$\phi_1,\ldots,\phi_K \in L_\phi$を無作為に選択し、Ｄａｎの公開鍵（$h_1,\ldots,h_K$）を使用して以下の計算を行う。

$$e \equiv \sum_{i=1}^{K} p\phi_i \otimes h_i + m \pmod q$$

これが、ＣａｔｈｙがＤａｎに送信する符号化メッセージである。

§１．４　復号

ＤａｎがＣａｔｈｙからメッセージｅを受信しており、自分の専用鍵ｆを使用してこのメッセージを復号するものと仮定する。これを効率的に行うために、Ｄａｎは第１．１節で説明した多項式Ｆを事前に計算しておくべきである。

ｅを復号するために、Ｄａｎはまず以下の計算を行う。

$$a \equiv f \otimes e \pmod q$$

この場合、Ｄａｎは－ｑ／２ないしｑ／２の間隔でａの係数を選択する。次に、Ｄａｎは、ａを整数係数を有する多項式とみなして、以下の計算を行うことによってメッセージを再生する。

$$F_p \otimes a \pmod p$$

注　パラメータ値が適切である場合、この復号手順によって最初のメッセージが再生される確率は極めて高い。しかし、ある種のパラメータ選択肢では、復号が失敗することがあり、したがっておそらく、各メッセージ・ブロックにいくつかの検査ビットを含めるべきである。復号が失敗する通常の原因は、メッセージのセンタリングが不適切であることである。この場合、Ｄａｎは、わずかに異なる間隔、たとえばｘがある小さな（正または負の）値である場合の－ｑ／２＋ｘないしｑ／２＋ｘで$a \equiv f \otimes e \pmod q$の係数を

選択することによってメッセージを回復することができる。ｘのどの値も機能しない場合には、間隔障害があり、メッセージを容易に復号することはできない。パラメータ値が適切に選択される場合に

は、間隔障害が起こることはまれであり、したがって、実際上間隔障害を無視することができる。

§１．５　なぜ復号が機能するか

Ｄａｎが計算した多項式ａは以下の数式を満たす。

$$a = f \otimes e = \sum_{i=1}^{k} f \otimes p\phi_i \otimes h_i + f \otimes m \pmod q$$
$$= \sum_{i=1}^{k} f \otimes p\phi_i \otimes F_q \otimes g_i + f \otimes m \pmod q \quad (2)\text{より}$$
$$= \sum_{i=1}^{k} p\phi_i \otimes g_i + f \otimes m \pmod q \quad (1)\text{より}$$

この最後の多項式について検討する。

$$\sum_{i=1}^{k} p\phi_i \otimes g_i + f \otimes m$$

パラメータの選択が適切である場合は、（ほぼ常に）すべての係数が－ｑ／２とｑ／２の間に位置し、したがって、ｑを法として係数が整約される場合でもこの多項式は変化しない。このことは、Ｄａｎが、ｑを法とするｆ⊗ｅの係数を－ｑ／２ないしｑ／２の間隔に整約するときに、以下の多項式を厳密に再生することを意味する。

$$Z[X] / (X^N-1) \text{ において } a = \sum_{i=1}^{k} p\phi_i \otimes g_i + f \otimes m$$

次いで、ｐを法としてａを整約すると、多項式ｆ⊗ｍ（ｍｏｄｐ）が与えられ、F_pによる乗算によってメッセージｍ（ｍｏｄｐ）が取り込まれる。

§２　パラメータの選択

§２．１　表記およびノルム推定

要素Ｆ∈Ｒの幅を次式のように定義する。

$$|F|_\infty = \max_{1 \le i \le N} \{F_i\} - \min_{1 \le i \le N} \{F_i\}$$

我々の表記が示すように、これは、Ｒ上の一種のＬ∞ノルムである。同様に、次式によってＲ上の対称Ｌ^{2}を定義する。

$$|F|_2 = \left(\sum_{i=1}^{N} (F_i - \bar{F})^2 \right)^{1/2} \qquad \text{ただし} \quad \bar{F} = \frac{1}{N} \sum_{i=1}^{N} F_i$$

（同様に、$|F|_2 / \sqrt{N}$はＦの係数の標準偏差である。）

前提　任意の$\varepsilon > 0$について、ε、Ｎ、Ｋに応じて定数ｃ１、ｃ２＞０があり、したがって、無作為に選択された多項式Ｆ１，．．．，Ｆκ、Ｇ１，．．．，Ｇκ∈Ｒについて、これらの多項式が次式を満たす確率は１－εよりも大きくなる。

$$c_1 \sum_{i=1}^{K} |F_i|_2 \cdot |G_i|_2 \le \left| \sum_{i=1}^{K} F_i \otimes G_i \right|_\infty \le c_2 \sum_{i=1}^{K} |F_i|_2 \cdot |G_i|_2 \qquad (3)$$

もちろん、この前提は、比ｃ２／ｃ１が小さなεに対して非常に大きい場合には、実際的な観点から無用である。しかし、ＮおよびＫが適度に大きな値を有し、εの値が非常に小さい場合でも、定数ｃ１、ｃ２が極端な値を有することはないことが判明している。このことは、実験によって多数の状況で検証されており、この論文において理論的な証拠の概要を示す。

§２．２　サンプル空間

典型的なサンプル空間の例として以下のものを使用する。

Ｌε＝｛ｇ∈Ｒ：ｇは－（ｒ－１）ないし（ｒ－１）／２の係数を有する｝

Ｌφ＝｛φ∈Ｒ：φは、１に等しいｄ個の係数と、－１に等しいｄ個の係数を有し、残りは０である｝

Ｌｍ＝｛ｍ∈Ｒ：ｍは－（ｓ－１）ないし（ｓ－１）／２の係数を有する｝

後で、セキュリティを達成するためにｒ、ｄ、ｓが満たさなければならない様々な制約があることが理解されよう。また、あらゆるφ

∈L_ϕがL^2ノルム$|\phi|_2=\sqrt{2d}$を有し、それに対して、平均要素$g\in L_g$および$m\in L_m$がL^2ノルム$|g|_2=\sqrt{N(r^2-1)/12}$および$|m|_2=\sqrt{N(s^2-1)/12}$を有することにも留意されたい。表記を容易に

するために、L_g、L_ϕ、L_mの要素の平均L^2ノルムをL_g、L_ϕ、L_mと書くことにする。

厳密に必要なことではないが、$L_m=pL_\phi$という追加の仮定を行

う。この仮定によって、可能な格子アタックを分析すると共に、そのようなアタックを有効でなくすことが容易になる。一例として、

$d=N/4$を選択すると仮定する。この場合、$s=\sqrt{6}p$が選択され

る。したがって、無作為にmの係数にpを加算し、mの係数からpを減算することによって、mに含まれる固有ｍｏｄ　ｐ情報の「密度を高くする」必要がある。

§２．３　復号基準

§１．５で説明したように、$|\Sigma p\phi_i\otimes g_i+f\otimes m|_\infty<q$であ

る場合、Ｄａｎは符号化メッセージmを復号することができる。上記の前提の不等式（３）を使用して（Kの代わりにＫ＋１を用い、εとして十分に小さな値を選択する）以下の推定を行うことができる。

$$\left|\sum_{i=1}^{K}p\phi_i\otimes g_i+f\otimes m\right|_\infty\leqq c_2\sum_{i=1}^{K}p|\phi_i|_2\cdot|g_i|_2+|f|_2\cdot|m|_2$$
$$\approx c_2L_g(KpL_\phi+L_m)$$
$$\approx c_2pL_gL_\phi(K+1)\quad(L_m\approx pL_\phi\text{と仮定})$$

したがって、（確率$1-\varepsilon$で）復号を行うために、Ｄａｎは、以下の復号制約を満たすパラメータを選択する必要がある。

$$c_2pL_gL_\phi\quad(K+1)<q\qquad(4)$$

§３　セキュリティ分析

§３．１　Ｍｅｅｔ－ｉｎ－ｔｈｅ－ｍｉｄｄｌｅアタック

説明を簡単にするために（かつアタッカを助けるために）、Ｋ＝１であり、したがって、符号化メッセージがｅ≡φ⊗ｈ＋ｍ（ｍｏｄ　ｑ）として表されるものと仮定する。Ａｎｄｒｅｗ　Ｏｄｌｙｚｋｏは、φに対して使用することのできるｍｅｅｔ－ｉｎ－ｔｈｅ－ｍｉｄｄｌｅアタックがあると指摘しており、専用鍵ｆにも同様なアタックが適用されると考えられる。簡単に言えば、ｆをｆ＝ｆ１＋ｆ２に分割し、ｆ１⊗ｅをｒ－ｆ２⊗ｅと突き合わせ、対応する係数がほぼ同じ値を有するような（ｆ1、ｆ2）を見つける。したがって、（たとえば）２８０のセキュリティ・レベルを得るには、約２160個の要素を含む集合からｆ、ｇ、φを選択しなければならない。

§３．２　多重送信アタック

やはり説明を簡単にするために、Ｋ＝１と仮定する。Ｃａｔｈｙが、同じ公開鍵と異なるランダムφを使用して単一のメッセージｍを数回にわたって送信する場合、アタッカＢｅｔｔｙは、メッセージの大部分を再生できると考えられる。簡単に言えば、Ｃａｔｈｙがｅｉ≡φｉ⊗ｈ＋ｍ（ｍｏｄ　ｑ）（ｉ＝１．２,...,ｒ）を送信すると仮定した場合、Ｂｅｔｔｙは（ｅｉ－ｅｉ）⊗ｈ－１（ｍｏｄ　ｑ）を計算し、それによってφi－φi（ｍｏｄ　ｑ）を再生することができる。しかし、φの係数は非常に小さいので、Ｂｅｔｔｙはφi－φiのみを再生し、これからφiの多数の係数を再生する。ｒが適度なサイズ（たとえば、４または５）である場合でも、Ｂｅｔｔｙは、ｂｒｕｔｅ　ｆｏｒｃｅによってすべての可能性を試験

するのに十分なφiを再生し、それによってｍを再生する。したがって、基本メッセージの他の何らかのスクランブリングを行わずに多重送信を行うことは好ましくない。Ｂｅｔｔｙが単一のメッセージをこのように復号する場合でも、この

情報は、他のメッセージを復号するうえで助けとならないことに留意されたい。

§３．３　格子ベースのアタック

まず格子整約に関するいくつかの語について説明する。格子整約の目標は、所与の格子M内の１つまたは複数の「小さな」ベクトルを見つけることである。理論的には、M内の最小のベクトルはしらみつぶし的探索によって見つけることができるが、実際には、Mの次元が大きい場合、これは不可能である。Ｓｃｈｎｏｒｒ［１１、１２］およびその他によって様々な改良を施されたＬｅｎｓｔｒａ－Ｌｅｎｓｔｒａ－Ｌｏｖａｓｚ［８］のＬＬＬアルゴリズムでは、多項式時間でMの最小ベクトルが見つかるが、次元の大きな（たとえば、≧１００）たいていの格子では、最小ベクトルは見つからず、最小のＬＬＬ判定可能ベクトルと実際の最小ベクトルとの間のギャップは次元と共に指数関数的に増加するようである。格子アタックに対するＮＴＲＵのセキュリティについて説明するために、大きな次元の格子に関する以下の３つの仮説を考える。

（H_1）たいていの格子Mでは、Mの最小非ゼロ・ベクトルの長さσ（M）は次式を満たす。

$$\sqrt{\frac{\dim(M)}{2\pi e}}\,\mathrm{Disc}(M)^{1/\dim(M)} \leqq \sigma(M) \leqq \sqrt{\frac{\dim(M)}{\pi e}}\,\mathrm{Disc}(M)^{1/\dim(M)}$$

したがって、$v \in M$が次式を満たす場合、

$$|v| \geqq \sqrt{\frac{\dim(M)}{\pi e}}\,\mathrm{Disc}(M)^{1/\dim(M)}$$

vはほぼ同じ長さの指数関数的に多数のベクトルに隠される。（H_2）格子Mが、（H_1）によって説明した予期される最短ベクトルよりも小さなベクトルwを有するが、他の場合には「ランダムな」格子であるものと仮定する。wが次式を満たす場合、

$$|w| \geqq \kappa^{-\dim(M)} \sqrt{\frac{\dim(M)}{\pi e}}\,\mathrm{Disc}(M)^{1/\dim(M)}$$

格子整約によってwが見つかる可能性は非常に低い。

（H_3）（H_2）の状況であると仮定する。この場合、格子整約方法によって算出される最小非ゼロ・ベクトルv_{LLL}はほぼ確実に次式を満たす。

$$|v_{LLL}| \geq K^{dim(M)} |w|$$

注　仮説（H_2）および（H_3）に現われる格子整約定数ｋは、実験および経験によって決定しなければならない。これは、ＲＳＡＰＫＣＳを用いた場合と同様であり、セキュリティは、積ｐｑを因数分解する現在の機能の推定に依存する。これは、［５］に記載されたＰＫＣＳにより類似しており、ＰＫＣＳのセキュリティは、格子の小さな（ほぼ直交化された）基を見つけるのが困難なことに直接関連している。次元の大きな（≧１００）格子を用いた実験によって、$K=1.5^{1/100}$を使用できることがわかっている。（たとえば、［１１］および［１２］を参照されたい。）因数分解が進むにつれて、ＲＳＡ　ＰＫＣＳで大きな素数を使用することが必要になり、したがって、格子の整約が進むにつれて、より小さな値のｋとそれに対応するより大きなパラメータをＮＴＲＵで使用することが必要になるのは間違いない。また、７００よりも大きな次元の格子については仮説（H_2）および（H_3）を仮定するだけでよい。このような高次元の格子では、場合によってはＳｃｈｎｏｒｒのブ

ロック整約改良を含むＬＬＬアルゴリズムでも長時間を必要とする。次元が約３００の格子について仮説（H_2）および（H_3）を仮定する場合、ずっと優れた動作特性を有するＮＴＲＵパラメータを選択することができる。

§３．３．１　鍵ｆに対する小格子アタック

まず、恐らく最も自然な格子から始め、すなわち、任意の１つの

ｈｉを選択し、ｈｉ⊗ｆ（ｍｏｄ　ｑ）も小さいという特性を有する

小さなベクトルｆを探索する。これを行うには、ｈｉ＝［$h_{i1},\ldots,h_{iN}$］とし、以下の行列の列によって生成される格子Ｍを検討する。

$$M=\left(\begin{array}{cccc|cccc} \lambda & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ 0 & \lambda & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda & 0 & 0 & \cdots & 0 \\ \hline h_{i1} & h_{i2} & \cdots & h_{iN} & q & 0 & \cdots & 0 \\ h_{i2} & h_{i3} & \cdots & h_{i1} & 0 & q & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ h_{iN} & h_{i1} & \cdots & h_{i,N-1} & 0 & 0 & \cdots & q \end{array}\right)$$

将来の表記に関する都合上、この行列を次式のように書く。

$$M=\begin{pmatrix} \lambda I & 0 \\ \overline{h}_i & qI \end{pmatrix}$$

アタックを最適化するためにアタッカによって数量λが選択される。

Mは次式を満たすと考えられる。

$$\mathrm{dim}\ (M)\ =2N\text{および}\mathrm{Disc}\ (M)\ =\lambda^N q^N$$

考慮すべき２つの問題がある。第１の問題は、Mに短いベクトルとして埋め込まれる実際の鍵ｆである。Mが以下の目標ベクトルを含み、

$$v_{targ}0=\ [\lambda f_N,\ldots,\lambda f_1,\ g_{i1},\ldots,g_{iN}]$$

v_{targ}がわかることによってｆを再生できることに留意されたい。しかし、ｖｔａｒｇの長さを次式のように算出することができる。

$$\left|v_{t=g}\right|_2=\sqrt{\left|\lambda f\right|_2^2+\left|g_i\right|_2^2}=L_g\sqrt{\lambda^2+1}$$

仮説（H_1）によれば、｜ｖｔａｒｇ｜$_2$が以下の不等式を満たす場合、ｆはアタックを受けても安全である。

$$\left|v_{t=g}\right|_2\geqq\sqrt{\frac{\dim(M)}{\pi e}}\mathrm{Disc}(M)^{1/\dim(M)}=\sqrt{\frac{2N\lambda q}{\pi e}}$$

言い換えれば、次式が成立する必要がある。

$$L_g\sqrt{\lambda+\lambda^{-1}}\geqq\sqrt{\frac{2Nq}{\pi e}}$$

アタッカは左辺を最小化したいので、アタッカの視点からの最適なλは$\lambda=1$（

補題A．１参照）である。したがって、次式が成立する場合は安全である。

$$q \leqq \frac{\pi c L_f^2}{N} \qquad (5)$$

考慮すべき第２の点は、M内の他のある小さなベクトルによって、アタッカがメッセージを復号できるかどうかである。したがって、

任意の小さなベクトル［ｆ’．ｇ’］∈Ｍは、ｆ’とｈｉ⊗ｆ’≡ｇ’（ｍｏｄ　ｑ）が共に小さいという特性を有する。しかし、アタッカが以下の計算を行った場合、

$$e \otimes f' = \sum_{j=1}^{K} p\phi_j \otimes h_j \otimes f' + m \otimes f' \pmod q$$

ｑを法とする小さな係数を有するのは、ｊ＝ｉを含む項だけである。したがって、単一のｈｉを小さくするｆ’は復号鍵としては働かない。このことは、すべてのｈｊを同時に検討していることを示し、

したがって次の格子に進む。

§３．３．　２　鍵ｆに対する大格子アタック

アタッカは、１つのｈｉのみを使用するのではなく、ｈｉのある部分集合を使用して格子を形成することができる。アタッカが、$h_1, \ldots, h_k$（$1 \leqq k \leqq K$）を使用し、以下の行列の列によって生成される格子Ｍを形成するものと仮定する。

$$\begin{pmatrix} \lambda I & 0 & 0 & 0 & \cdots & 0 \\ \overline{h}_1 & qI & 0 & 0 & \cdots & 0 \\ \overline{h}_2 & 0 & qI & 0 & \cdots & 0 \\ \overline{h}_3 & 0 & 0 & qI & \cdots & 0 \\ \vdots & & & & \ddots & \vdots \\ \overline{h}_k & 0 & 0 & 0 & \cdots & qI \end{pmatrix}$$

（前の節の略号を使用している）この格子は次式を満たす。

$dim(M) = (k+1)$ ＮおよびＤｉｓｃ（Ｍ）$= \lambda^N q^{kN}$

この格子は、（自明のショートハンドを使用する）目標ベクトルを含む。

$$v_{targ} = \{\lambda f, g_1, g_2, \ldots, g_k\}$$

（より厳密に言えば、ｆの座標を反転する必要がある。）この目標ベクトルは以下の長さを有する。

$$|v_{targ}|_2 = \sqrt{\lambda f|_2^2 + |g_1|_2^2 + \cdots |g_k|_2^2} = L_g\sqrt{\lambda^2 + k}$$

仮説（H_2）によれば、ｖｔａｒｇの長さが次式を満たしているかぎり、格子整約ではｖｔａｒｇを見つけることはできない。

$$|v_{targ}|_2 \geqq \kappa^{-\dim(M)}\sqrt{\frac{\dim(M)}{\pi e}}\mathrm{Disc}(M)^{1/\dim(M)}$$
$$= \kappa^{-(k+1)N}\sqrt{\frac{(k+1)N}{\pi e}}\cdot\lambda^{1/(k+1)}q^{k/(k+1)}$$

したがって、次式が成立する場合にはアタックを受けても安全であ

る。

$$L_g\sqrt{\lambda^{2k/(k+1)} + k\lambda^{-2/(k+1)}} \geqq \kappa^{-(k+1)N}\sqrt{\frac{(k+1)N}{\pi e}}q^{k/(k+1)}$$

前述のように、アタッカはλを選択して左辺を最小化する。この場合も、λ＝１の場合に最小値が得られ（補題Ａ．１参照）、したがって、次式が成立するかぎり仮説（H_2）の下で実際の鍵は安全である。

$$q^{k/(k+1)} \leqq \kappa^{(k+1)N}L_g\sqrt{\frac{\pi e}{N}} \qquad (6)$$

§３．３．３　スプリアス鍵ｆに対する大格子アタック

アタッカは、真の鍵ｆを探索するのではなく、復号鍵として働く他の何らかの鍵Ｆを見つけることを試みることがある。Ｆ自体と各積$h_j \otimes F \pmod q$をスプリアス鍵にするには、これらを小さくしなければならない。話を厳密にするために、アタッカがＦを見つけ次式を計算するものと仮定する。

$$G_j = h_j \otimes F \pmod q \quad (j = 1, 2, \ldots, K)$$

次式の幅（L∞ノルム）が一般に、

$$\phi_1 \otimes G_1 + \phi_2 \otimes G_2 + \ldots + \phi_K \otimes G_K + m \otimes F$$

あるラッピング係数Wについて少なくともWqであることを知る必要がある（システムが安全であるにはWをどのくらい大きくしなければならないかの問題については第４章で論じる）。

アタッカは、スプリアス鍵Fを見つけるために、第３．３．２節で説明した格子Mを取り出し、格子整約技法を使用して小さなベクトルvLLLを見つける。M内の最小非ゼロ・ベクトルはベクトルvtarg＝｛λf，g1，...，gK｝であり、したがって、仮説（H3）によれば次式が成立する。

$$|v_{LLL}|_2 \geqq k^{(K+1)N} |v_{targ}|_2$$

vLLL＝［λF，G1，G2，...，GK］とすると、次式が成立することがわかる。

$$\sqrt{\lambda^2|F|_2^2 + |G_1|_2^2 + \cdots + |G_K|_2^2} \geqq \kappa^{(K+1)N} L_g \sqrt{\lambda^2 + K}$$

格子整約によって得られるベクトルvLLLは、サイズが多少とも無作為に分散する成分を有する。特に、すべての長さ｜λF｜2，｜G1｜2，...，｜GK｜2がほぼ同じであり、したがって、（ほぼ）次式が得られる。

$$|\lambda F|_2, |G_1|_2, \ldots, |GK|_2 \geqq k^{(K+1)N} L_g$$

一方、これと（３）を使用して以下の推定を行うことができる。

$$\begin{aligned} |\phi_1 \otimes G_1 + \phi_2 \otimes G_2 + \ldots + \phi_K \otimes G_K + m \otimes F|_\infty \\ &\geqq c_1(|\phi_1|_2 \cdot |G_1|_2 + \ldots + |\phi_K|_2 \cdot |G_K|_2 + |m|_2 \cdot |F|_2) \\ &= c_1 L_\phi (|G_1|_2 + \ldots + |G_K|_2 + |F|_2) \\ &\geqq c_1(K+1) L_\phi L_g \kappa^{(K+1)N} \end{aligned}$$

したがって、ラッピング係数Wを用いた場合、パラメータとして次式を満たすパラメータが選択されるかぎり、スプリアス鍵を得ることはできない。

$$W_q \leqq c_1 (K+1) L_\phi L_g k^{(K+1)N} \quad (7)$$

（これを復号不等式（４）と比較することができる）

§３．３．４ 個々のメッセージに対する大格子アタック

考慮しなければならない他の種類の格子アタックがある。アタッカは、あらゆるメッセージを復号する鍵を探索するのではなく、個々のメッセージを探索する格子を構築することができる。以下の格子について考える。この格子は第３．３．２節で使用した格子に類似している。以下の行列の列によって生成される格子をＭとする。

$$\begin{pmatrix} \lambda I & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & \lambda I & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \lambda I & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \lambda I & \cdots & 0 & 0 \\ \vdots & & & & \ddots & & \vdots \\ \vdots & & & & & \ddots & \vdots \\ p\tilde{h}_1 & p\tilde{h}_2 & p\tilde{h}_3 & & \cdots & p\tilde{h}_K & qI \end{pmatrix}$$

この格子は次式を満たし、

ｄｉｍ（Ｍ）＝（Ｋ＋１）ＮおよびＤｉｓｃ（Ｍ）＝$\lambda^{KN} q^N$

以下のベクトルを含む(自明の表記を使用する)。

$$[\lambda\phi_1, \lambda\phi_2, \ldots, \lambda\phi_K, e-m]$$

この格子がこのベクトルを含むのは、符号化メッセージｅが以下の規則に従って作成されたからである。

$$p\phi_1 \otimes h_1 + p\phi_2 \otimes h_2 + \ldots + p\phi_K \otimes h_K + m \equiv e \pmod q$$

ｅ－ｍ（ｍｏｄ　ｑ）の係数が小さくないので（８）が短いベクトルになる可能性が低いことは明らかである。しかし、アタッカはｅの値を知っており、したがって、既知の非格子ベクトル［０，０，．．．，０，ｅ］に近いベクトルをＭで探索することができる。探索中の格子ベクトルおよび既知の非格子ベクトルからの距離は、以下のベクトルの長さである。

$$v_{targ} = [\lambda\phi_1, \lambda\phi_2, \ldots, \lambda\phi_K, -m]$$

これは、非斉次格子問題の例である。非斉次問題は斉次問題よりもいくらか難しくなる傾向があるが、重大な誤りを犯すのを回避するために、アタッカが非斉次問題を斉次問題を解くのとまったく同じ程度に解くことができると仮定する。したがって、アタッカが以下の長さのベクトルを見つけられるかどうかを調べる必

要がある。

$$|v_{1\wedge g}|_2 = L_\phi \sqrt{K\lambda^2 + p^2}$$

（あらゆるｍ∈L_mおよびあらゆるϕ E∈L_ϕについて｜ｍ｜$_2$＝ｐ

｜ϕ｜$_2$であることを想起されたい）仮説（H_2）によれば、次式が成立する場合

$$|v_{1\wedge g}| \geqq K^{-\dim(M)} \sqrt{\frac{\dim(M)}{\pi e}} \mathrm{Disc}(M)^{1/\dim(M)}$$

あるいは言い換えれば、次式が成立する場合には、アタックは失敗する。

$$L_\phi \sqrt{K\lambda^{2/(K+1)} + p^2 \lambda^{-2K/(K+1)}} \geqq K^{-(K+1)N} \sqrt{\frac{(K+1)N}{\pi e}} q^{1/(K+1)}$$

アタッカは、$\lambda = p$（補題Ａ．１参照）を使用することによって左辺を最小化し、したがって、次式が成立する場合、アタックは失敗する。

$$q^{1/(K+1)} \leqq K^{(K+1)N} L_\phi \sqrt{\frac{\pi e}{N}} p^{1/(K+1)} \qquad (9)$$

この数式は、これによって補われる（６）と比較することができる。

§３．３．５　格子アタック・パラメータ制約の要約

本節の前の部分では、様々な格子アタックについて説明し、これらのアタックが成功するのを妨げる、パラメータに対する制約を考案した。すべての制約を満たすパラメータの選択肢が存在するかどうかという問題が残っている。読者に好都合なように、本節のすべての不等式を、真の鍵ｆの所有者がメッセージを復号する場合に必要な基本不等式（４）と共にリストする。

$$c_2 p L_g L_\phi (K+1) < q \qquad (4)$$

$$q \leqq \frac{\pi e L_g^2}{N} \qquad (5)$$

$$q^{k/(k+1)} \leqq K^{(k+1)N} L_g \sqrt{\frac{\pi e}{N}} \quad （１\leqq k \leqq K の全てに対して） \qquad (6_k)$$

$$W_q \leqq c_1 (K+1) L_\phi L_g^{K^{(K+1)N}} \tag{7}$$

$$q^{1/(K+1)} \leqq K^{(K+1)N} L_\phi \sqrt{\frac{\pi e}{N}} p^{1/(K+1)} \tag{9}$$

任意の固定値c_1、c_2、p、$L_\phi > 0$であり、p、k、$W > 1$である場合、これらの不等式には常に解N、k、L_g、qが存在すると考えられる。次に、解を求める際に助けとなるいくつかの注意事項について述べる。

まず、これらの不等式を様々な方法で組み合わせる。まず、（４）と（７）を組み合わせると（ある代数計算の後で）次式が与えられる。

$$(K+1)N \geqq \frac{\log (c_1^{-1} c_2 p W)}{\log K} \tag{10}$$

（基本的に）c_1、c_2、kを自由に選択することはできず、Wが所望のセキュリティ・レベルに応じて５と１０の間で選択されることに留意されたい。これによって、通常はかなり小さなpが選択される。この場合の重要な点は、（１０）が（Ｋ＋１）Ｎの下限を与え、これを超えるとほとんど制御できなくなることである。

次に、（４）と（５）を組み合わせると次式が得られる。

$$L_g > \frac{c_2 p (K+1) N}{\pi e} L_\phi \tag{11}$$

qを選択する際にいくらか融通を利かせるには、L_gの値として、指定されたこの下限よりも（たとえば）１．５倍ないし２倍大きな値を選択するとよい。

たとえば、L_ϕおよびL_gが第２．２節で説明したような値である場合、$L_\phi = \sqrt{2d}$であり、大部分の$g \in L_g$は$|g|_2 \sim L_g = \sqrt{N(r^2-1)/12}$を満たす。したがって、（１１）を使用して$L_g$を選択した後、$r = \lfloor L_g \sqrt{12/N} \rfloor$を選択することができ、この場合、大部分の$g \in L_g$は所望の$L_g$に非常に近い$L^2$ノルムを有する。さらに、$L_g$から要素を選択するのは符号作成者のＤａｎだけであり、このような選択は１度行うだけ

でよいので、Ｄａｎが、ほぼL_gのノルムを有するL_gで必要なＫ＋１個の多項式を見つけるのは難しいことではない。長さの制約がある場合でも、実際にはr^Nが少なくとも2500になる傾向があるので、L_g内のそのような多項式の数はアタッカがしらみつぶし的探索を介して検査できるよりもはるかに多い。

§４　実施にあたって考慮すべき点

§４．１　セキュリティ係数およびラッピング係数

アタッカが、格子整約によって生成されたスプリアス鍵を使用するときにどの程度のラッピングを期待できるかを、ラッピング係数Ｗが制御することを想起されたい。Ｗが小さすぎ、たとえばＷ＝１．５である場合、アタッカは多数の（場合によっては最も多くの）係数を回復することができる。これは、これらの値が平均の周りに集中する傾向があるからである。厳密には、アタッカはＮ個の未知の係数に関して（たとえば）０．９５Ｎ個の一次方程式を再生し、この場合、暴力的探索によってアタックが終了する。

ＣｏｐｐｅｒｓｍｉｔｈおよびＳｈａｍｉｒ［３］は、Ｗがこれよりも大きなビットであり、たとえばＷ＝２．５である場合でも、アタッカはクラスタ化により、Ｎ個の未知の係数について約０．６７Ｎ個の一次方程式を得ることができると考えた。ＣｏｐｐｅｒｓｍｉｔｈおよびＳｈａｍｉｒは次いで、アタッカが２つの独立のスプリアス鍵を構築し適用した場合、システムの解を求めるのに十分な数の独立の等式を得ることができると考えている。ＣｏｐｐｅｒｓｍｉｔｈおよびＳｈａｍｉｒはさらに、Ｗ＝４である場合、いくつかの短いベクトルを使用し、ある種の誤り補正技法を使用することによって、アタックを成功させることができるが、Ｗが１０程度である場合には、この種のアタックは成功しないと述べている。詳細については［３］を参照されたい。

これらのことに基づいて、ラッピング係数Ｗ＝１０を使用してサンプル動作パラメータを構築する。

§４．２　サンプル動作パラメータ

この節では、第３節の仮説の下で安全であるＮＴＲＵ　ＰＫＣＳの２組の使用可能なパラメータを考案する。これらのパラメータ集合によってかなり高度なメ

ッセージ拡張が行われ、したがって、メッセージ拡張を管理可能な２対１に低減するＮＴＲＵの２段階バージョンに関する以下の第４．３節を参照されたい。

まず、実験による証拠によって得られた３つの値と、スプリアス鍵アタックを妨げるのに十分なラッピングが確保されるように選択された第４の値から始める。

$c_1=0.08,\quad c_2=0.24,\quad W=10\quad \kappa=1.5^{1/100}\approx 1.0040628823$

c_1およびc_2の値は所望の範囲の広範囲な数値試験によって決定されているが、これらの値を確率的に正当化するにはどうすべきかについてかなり良好な考え方がある。上記の第４．１節でラッピング係数Ｗ＝１０について論じた。最後に、第３．３節の注で格子整約定数κの選択について論じた。ただし、格子整約技法の将来の改良に備えるために、セキュリティを意識するユーザはこの代わりに$\kappa=1.3^{1/100}$を選択し、他のパラメータをわずかに変更することができる。

まず選択肢ｐ＝２について考える。第３．３．５節の不等式（１０）によって、次式を選択する必要があることがわかる。

$$(K+1)\ N \geqq 1009.79$$

したがって、以下の値を選択する。

$$N=167 \text{ および } K=6$$

（Ｎと（Ｎ－１）２が共に素数であると好都合である。ただし、これは必要なことではない）。この選択によって、残りの係数を選択するための十分な許容差が与えられる。

L_ϕを第２．２節と同様に選択し、ｄ＝２０とし、したがって、

$\#L_\phi=167!/20!\cdot 20!\cdot 127!\approx 2^{155.85}$となる。

これはｍｅｅｔ－ｉｎ－ｔｈｅ－ｍｉｄｄｌｅアタックに対する十分なセキュリティを与える。さらに、$L_\phi=\sqrt{2d}\approx 6.325$とし、

これらの選択肢を（１１）に代入すると、$L_E>414.07$が与えられる。い

くらかの許容差を与えるためにγ＝１６７を選択する。これによって、L_gの期待値は６２２．９８に等しくなる。最後に、第３．３．５節の５つの基本不等式により、ｑが次式を満たさなければならないことがわかる。

$$2^{13.6924} < q \leq \max\{2^{14.2766}, 2^{14.7278}, 2^{14.6238}, 2^{52.481}\}$$

（もちろん、第３．３．５節の不等式（６ｋ）は実際には、各１≦ｋ≦６ごとに１つの６つの不等式である。）したがって、ｑ＝2^{14}－１＝１６３８３を選択することができる。（ｇｃｄ（ｐ，ｑ）＝１が必要であることに留意されたい。）簡単に言えば、第３．３節の仮説を仮定した場合、以下のパラメータによって安全なＮＴＲＵＰＫＣＳが与えられる。

$$N=167,\ k=6,\ q=16383=2^{14}-1,\ p=2,\ r=167,\ d=20,\ s=3$$

この場合、第２．２節で説明したように、L_ϕ、L_g、L_mが選択

される。これらのパラメータでは以下の値が得られる。

公開鍵長＝Ｎｋｌｏｇ$_2$ｑ＝１４０２８ビット

専用鍵長＝Ｎｌｏｇ$_2$ｐｒ＝１４００ビット

メッセージ拡張＝ｌｏｇｑ／ｌｏｇｐ＝１４対１

同様な分析を使用して、より大きな値のｐを有する第２の１組の安全なＮＴＲＵパラメータを構築する。すべての演算が2^{16}よりも小さな数に対して行われ、ｑが２のべき乗であり、したがって、剰余を含むｑによる除算が簡単なシフト演算になるので、これらのパラメータは既存のマイクロプロセッサにうまく適合するように思われる。以下の値を選択する。

$$N=167,\ K=6,\ q=2^{16},\ p=3,\ r=354,\ d=40,\ s=7$$

これらのパラメータは$\#L_\phi$＝１６７！／４０！・４０！・８７！

$\approx 2^{239.3}$と、以下の値を与える。

公開鍵長＝ＮＫｌｏｇ$_2$ｑ＝１６０３２ビット

専用鍵長＝Ｎｌｏｇ$_2$ｐｒ＝１６７８ビット

メッセージ拡張＝ｌｏｇｑ／ｌｏｇｐ＝１０．１対１

§４．３　２段階ＮＴＲＵおよび改良型メッセージ拡張

第４．２節に示したサンプル・パラメータのＮＴＲＵ　ＰＫＣＳはかなり大き

なメッセージ拡張を有する。この拡張を減少する１つの方法は、より大きな値のｐを使用することであるが、この場合、（Ｋ＋１）Ｎの値が著しく大きくなり、そのため両方の鍵サイズが大きくなり計算効率が低下する。

メッセージ拡張を減少する他の方法は、実際のメッセージを符号化するための１種のワンタイム・パッドとして各ＮＴＲＵメッセージを使用することである。ＮＴＲＵのこの２段階バージョンでは、符号化側のＣａｔｈｙがランダム多項式$m \in L_m$を選択し、これに

対して、Ｃａｔｈｙの実際の平文メッセージＭとしては、ｑを法とする任意の多項式が許容される。Ｃａｔｈｙは、メッセージを符号化するために、以下の２つの等式を計算する。

$$e \equiv \sum_{i=1}^{K} p\phi_i \otimes h_i + m \pmod q \text{ および } E \equiv m \otimes h_1 + M \pmod q$$

符号化メッセージは対（ｅ，Ｅ）である。

復号プロセスは前述のプロセスと類似しているが、１つの余分のステップを含む。したがって、復号側のＤａｎは、第１．４節で説明した手順に従って多項式ｍを計算する。Ｄａｎは次いで、次式を計算することによってメッセージを再生する。

$$E - m \otimes h_1 \pmod q$$

平文メッセージＭの長さが$N \log_2 q$ビットであり、それに対して符号化メッセージ（ｅ，Ｅ）の長さが$2N \log_2 q$ビットであり、したがってメッセージ拡張は２対１に減少すると考えられる。

別の点について述べる。Ｃａｔｈｙは同じ多項式および法を使用してｍとＭの両方を符号化している。これによってセキュリティが損なわれることは考えられないが、セキュリティを強化した場合、

Ｃａｔｈｙは異なる（公開）多項式Ｈおよび法Ｑについて$E \equiv m \otimes H + M \pmod q$を計算することができる。

§４．４　理論上の動作仕様

この節では、ＮＴＲＵ　ＰＫＣＳの理論上の動作特性について考える。４つの

整数パラメータ（N、K、p、q）と、第２．２節で説明したように、それぞれ、整数r、d、sによって決定される、３つの集合L_g、L_ϕ、L_mと、実験的に決定される定数c_1、c_2、kと、ラッピング定数Wがある。セキュリティを保証するには、こ

れらのパラメータとして、第３．３．５節にリストした不等式を満たすパラメータを選択しなければならない。以下の表は、これらのパラメータで表したＮＴＲＵ　ＰＫＣＳ動作特性を要約したものである。

平文ブロック	$N \log_2 p$ビット
符号化テキスト・ブロック	$N \log_2 q$ビット
符号化速度*	$O(KN^2)$回の演算
復号速度	$O(N^2)$回の演算
メッセージ拡張	$\log_p q$対１
専用鍵長	$N \log_2 p r$ビット
公開鍵長	$KN \log_2 q$ビット

＊厳密には、$4KN^2$回の加算と、KN回の、剰余を含むqによる除算

第４．４節で説明した２段階ＮＴＲＵについては以下の項目が異なる。

平文ブロック	$N \log_2 q$ビット
符号化テキスト・ブロック	$2N \log_2 q$ビット
メッセージ拡張	２対１

§４．５　実施上の他の考慮すべき点

ＮＴＲＵを実施する際に考慮すべき他のいくつかの因子について簡単に述べる。

（１）ｇｃｄ（ｑ，ｐ）＝１であることが重要である。基本的にＮ

ＴＲＵはこの要件がなくても働くが、実際には、ｇｃｄ（ｑ，ｐ）＞１である場合、セキュリティが低下する。極端な範囲では、ｐ｜ｑである場合、（ｅｘｅｒ

ｃｉｓｅ）符号化メッセージｅはｅ≡ｍ（ｍｏｄ　ｐ）を満たし、ＮＴＲＵのセキュリティは完全に失われる。

（２）大部分のｆがｐおよびｑを法とする逆数を有することが望ましい。というのは、そうでない場合、鍵の作成が困難になるからである。第１の要件はｇｃｄ（ｆ（１），ｐｑ）＝１であるが、これが、ある選択されたｆに対して無効であった場合、符号作成者はこの代わりにたとえば、ｆ（Ｘ）＋１またはｆ（Ｘ）－１を使用することができる。ｇｃｄ（ｆ（１），ｐｑ）＝１と仮定すると、Ｎとして素数を選択し、ｐおよびｑを除する各素数Ｐについて、（Ｚ／ＮＺ）*中のＰのオーダーを大きくし、たとえばＮ－１または（Ｎ－１）／２にした場合、ほぼすべてのｆ、が必要な逆数を有する。たとえば、これは、（Ｎ－１）／２自体が素である（すなわち、ＮがＳｏｐｈｉｅ　Ｇｅｒｍａｉｎ素数である）場合は確実に真である。このような素数の例には１０７および１６７が含まれる。

§５　ＮＴＲＵの適度なセキュリティ・パラメータ

現実には、高速および／または低メモリ要件が重要であり、適度なセキュリティ・レベルが受け入れられる多数の状況がある。この場合、実際の格子整約方法［１１、１２］はＣＰＵを酷使し、そればかりでなく、次元２００ないし３００の格子に対して格子整約を実行するのに長いコンピュータ時間を必要とする。もちろん、この場合の「長い」は相対的な語であるが、３００次元格子整約を実行して１セントの数分の１に相当するコストを削減しても恐らく無効であり、現行の方法を使用してこのような格子整約を短時間（たとえば２、３分間）で実行すると（完全に実現不能ではない場合）コストが非常に高くなることは確実である。したがって、大次元格子アタックを可能にする必要のある状況で使用できる１組のＮＴＲＵパラメータを作成すると有効である。

格子アタックによってもたらされるパラメータ制約をなくした場合、残るのは以下の復号制約と、

$$c_2 p L_g L_\phi \quad (K+1) < q \qquad (4)$$

ｆ、ｇ、φの探索空間が暴力的（多分ｍｅｅｔ－ｉｎ－ｔｈｅ－ｍｉｄｄｌｅ）アタックを防止するほど大きいという条件だけである。話を簡単にするために、

Ｋ＝１を選択する。ｆ、ｇ、φがすべて、集合Ｌφ、すなわち、ｄ個の係数が１に等しく、ｄ個の係数が－１に等しく、他のＮ－２ｄ個の係数が０に等しい多項式の集合に含まれるものとみなす。（厳密には、ｆはｐおよびｑを法として可逆である必要があるので、ｆを余分の１つの係数を有するものとみなすが、これは後に続く分析にほとんど影響を与えず、したがってこれを無視することにする。）ｃ２＝０．２４を通常どおりに使用すると、復号制約は単に次式のようになる。

$$q > 2pd \qquad (4)$$

他の制約を次式に示す。

$$\binom{N}{d;\, d;\, N-2d} = \frac{N!}{(d!)^2(N-2d)!} \geq 2^{2\sigma}$$

上式で、σは必要なセキュリティ・レベルである。適度なセキュリティの処理系の場合、セキュリティ・レベルは約2^{40}でほぼ十分

であり、したがってσ＝４０を選択する。

以下の表は、ＮＴＲＵの適度なセキュリティの処理系の受け入れられる動作パラメータを示す。セキュリティを評価する際、利用可

能な格子アタックが次元２Ｎの格子を使用することに留意されたい。また、ｑのリストされた値は最小許容値であるが、ｇｃｄ（ｐ，ｑ）を満たす、これよりもいくらか大きなｑも受け入れられることに留意されたい。特に、ｑ＝６４を選択することによってとりわけ高速な処理系を使用することができる。

N	d	σ	p	q
107	9	41.11	2	37
107	9	41.11	3	55
167	7	38.98	2	29
167	7	38.98	3	43
263	7	43.72	2	29
263	7	43.72	3	43

最後に、鍵サイズが非常に小さくなると考えられる。

公開鍵：$N\log_2(q)$ビット

専用鍵：$2N\log_2(p)$ビット

たとえば、$(N, d, p, q) = (167, 7, 3, 64)$は、それぞれ長さ１００２ビットおよび５３０ビットの公開鍵および専用鍵を含むシステムを形成する。

§６　他のＰＫＣＳとの比較

現在、因数分解の難点に基づくＲｉｖｅｓｔ、Ｓｈａｍｉｒ、Ａｄｅｌｍａｎ（ＲＳＡ［１０］）のシステム、誤り補正符号に基づくＭｃＥｌｉｅｃｅ［９］のシステム、ほぼＶ直交化された短い基を格子内で見つけることが困難であることに基づくＧｏｌｄｒｅｉｃｈ、Ｇｏｌｄｗａｓｓｅｒ、Ｈａｌｅｖｉ（ＧＧＨ［５］）の最近のシステムを含め、いくつかの公開鍵暗号システムが文献に記載されている。

ＮＴＲＵシステムは、環Ｒ内の星印乗算を（特殊な種類の）行列の乗算として公式化することができ、次いで、システムでの符号化を行列乗算$E = AX + Y$（Ａは公開鍵である）として書くことができるという点で、ＭｃＥｌｉｅｃｅのシステムと共通するいくつかの特徴を有する。２つのシステムの間の小さな違いは、ＮＴＲＵ符号化では、Ｙがメッセージであり、Ｘがランダム・ベクトルであるが、ＭｃＥｌｉｅｃｅシステムではこれらの割当てが逆になることである。しかし、実際の違いは、復号を可能にする基本トラップドアである。ＭｃＥｌｉｅｃｅシステムの場合、行列Ａが誤り補正（ゴッパ）符号に関連付けされ、ランダム寄与がゴッパ符号によって「補正される」ほど小さいために復号が作用する。ＮＴＲＵの場合、行列Ａは巡回行列であり、復号は、Ａの、特殊な形式を有する２つの行列の積へ分解と、ｍｏｄ　ｑからｍｏｄ　ｐへのリフティングに依存する。

我々の知るかぎりでは、ＮＴＲＵシステムにはＲＳＡシステムとの共通点がほとんどない。同様に、ＮＴＲＵシステムは格子整約アタックを防止するようにセットアップしなければならないが、その基本復号方法は、復号が短い格子基の知識に基づいて行われるＧＧＨシステムとはかなり異なるものである。なお、ＧＧ

Hは実際には、ＭｃＥｌｉｅｃｅシステムに類似している。これは、どちらの場合でも、小さなランダム寄与を認識してなくすことによって復号が実行されるからである。これに対して、ＮＴＲＵは、可分性（すなわち、合同）を考慮することによってずっと大きなランダム寄与をなくす。

以下の表は、ＲＳＡ暗号システム、ＭｃＥｌｉｅｃｅ暗号システム、ＧＧＨ暗号システム、ＮＴＲＵ暗号システムのいくつかの理論的動作特性を比較したものである。それぞれの場合において、数Ｎは固有セキュリティ／メッセージ長パラメータを表す。

	NTRU	RSA	McEliece	GGH
符号化速度	N^2	N^2	N^2	N^2
復号速度	N^2	N^3	N^2	N^2
公開鍵	N	N	N^2	N^2
専用鍵	N	N	N^2	N^2
メッセージ拡張	2-1	1-1	2-1	1-1

付録Ａ．基本補題

以下の結果は格子アタックを最適化するうえで有用である。補題Ａ．１．$\alpha+\beta=1$を有するすべてのＡ、Ｂ、α、βについて、

$$\inf_{x>0} Ax^{\alpha}+Bx^{-\beta}=\frac{A^{\beta}B^{\alpha}}{\alpha^{\alpha}\beta^{\beta}}$$

が成立し、$x=\beta B/\alpha A$で下限が生じる。

証明　$f(x)=Ax^{\alpha}+Bx^{-\beta}$とする。この場合、$f'(x)=\alpha Ax^{\alpha-1}-\beta Bx^{-\beta-1}=x^{\beta+1}(\alpha Ax-\beta B)$である。したがって、絶対最小値は$x=\beta B/\alpha A$で生じる。　（$x\rightarrow 0^{+}$および$x\rightarrow\infty$のときに$f(x)\rightarrow\infty$であることに留意されたい。）

参考文献

１．M. Blum、S. Goldwasser 著「An efficient probabilistic public-key encryption scheme which hides all partial information」Advances in Cryptology: Proceedings of CRYPTO 84, Lecture Notes in Computer Science、第 196 巻、Splinger-Verlag、1985 年、289 ページ～299 ページ

２．H. Cohen 著「A course in computational algebraic number theory」Graduate Texts in Math、第 138 巻、Splinger Verlag、ベルリン、1993 年

３．D. Coppersmith、A. Shamir 著「Lattice attacks on NTRU」前刷り、1997 年 4 月 5 日、Eurocrypt 97 にて発表

４．W. Diffie、M. E. Hellman 著「New directions in cryptography」IEEE Trans. on Information Theory 22（1976 年）、644 ページないし 654 ページ

５．O. Goldreich、S. Goldwasser、S. Halevi 著「Public-key

cryptosystems from lattice reduction problems」 MIT-Laboratory for Computer Science 前刷り、1996 年 11 月

6．S. Goldwasser および A. Micali 著「Probabilistic encryption」J. Computer and Systems Science 28（1984 年）、270 ページないし 299 ページ

7．J. Hoffstein、J. Pipher、J.H. Silverman 著「NTRU: A new high speed public key cryptosystem、前刷り、Crypto 96 のランプ・セッションにて発表

8．A.K. Lenstra、H.W. Lenstra、L. Lovsz 著「Factoring polynominals with polynominal coefficients」Math. Annalen 261（1982 年）、515 ページないし 534 ページ

9．R.J. McEliece 著「A public-key cryptosystem based on algebraic coding theory」、JPL Pasadena, DSN Progress Reports 第 42 巻ないし第 44 巻（1978 年）、114 ページないし 116 ページ

10．R.L. Rivest、A. Shamir、L. Adleman 著「A method for obtaining digital signatures and public key cryptosystems」Communications of the ACM 21（1978 年）、120 ページないし 126 ページ

11．C.P. Schnorr 著「Block reduced lattice bases and successive minima」Combinatorics, Probability and Computing 3（1994 年）、507 ページないし 522 ページ

12．C.P. Schnorr、H.H. Hoerner 著「Attacking the Chor Rivest cryptosystem by improved lattice reduction」Proc. EUROCRYPT 1995, Lecture Notes in Computer Science 921、Springer-Verlag、1995 年、1 ページないし 12 ページ

13．D. Stinson 著「Cryptography: Theory and Practice」CRC Press、Boca Raton、1995 年

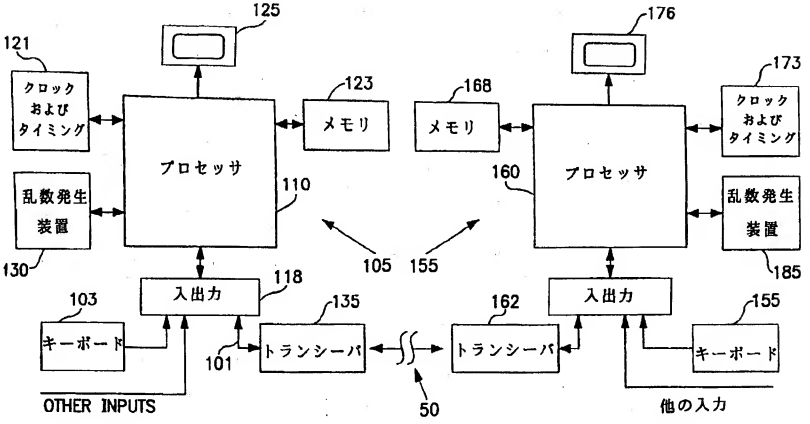

125
121
クロック
および
タイミング
123
メモリ
プロセッサ
110
乱数発生
装置
130
105
155
168
メモリ
176
173
クロック
および
タイミング
160
プロセッサ
乱数発生
装置
185
118
入出力
103
キーボード
135
トランシーバ
101
OTHER INPUTS
50
162
トランシーバ
入出力
155
キーボード
他の入力

FIG. 1

【図２】

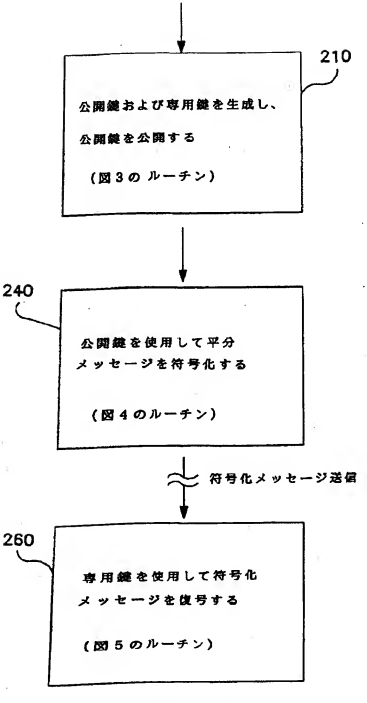

210
公開鍵および専用鍵を生成し、
公開鍵を公開する
（図３のルーチン）
240
公開鍵を使用して平分
メッセージを符号化する
（図４のルーチン）
符号化メッセージ送信
260
専用鍵を使用して符号化
メッセージを復号する
（図５のルーチン）

FIG. 2

【図３】

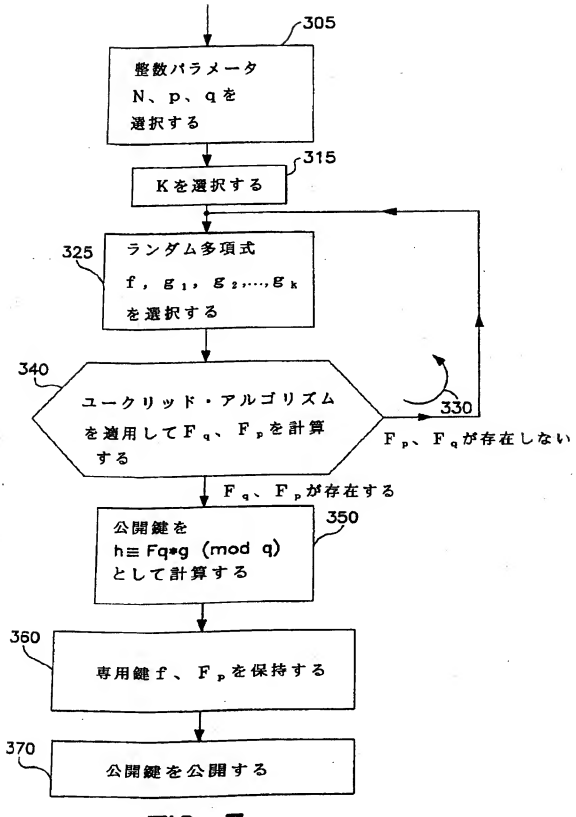

305
整数パラメータ
N、p、qを
選択する
315
Kを選択する
325
ランダム多項式
f, g1, g2,…,gk
を選択する
340
ユークリッド・アルゴリズム
を適用してFq、Fpを計算
する
330
Fp、Fqが存在しない
Fq、Fpが存在する
350
公開鍵を
h≡Fq*g (mod q)
として計算する
360
専用鍵f、Fpを保持する
370
公開鍵を公開する

FIG. 3

【図４】

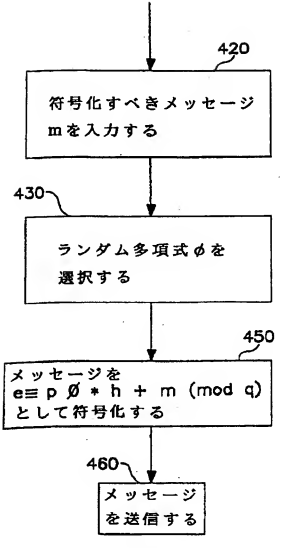

420
符号化すべきメッセージmを入力する
430
ランダム多項式φを選択する
450
メッセージを e≡ p Ø * h + m (mod q) として符号化する
460
メッセージを送信する

FIG. 4

【図５】

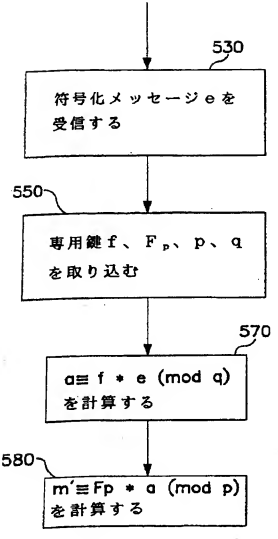

530
符号化メッセージｅを
受信する
550
専用鍵ｆ、Ｆｐ、ｐ、ｑ
を取り込む
570
ａ≡ｆ＊ｅ (mod ｑ)
を計算する
580
ｍ′≡Ｆｐ＊ａ (mod ｐ)
を計算する

FIG. 5

【図６】

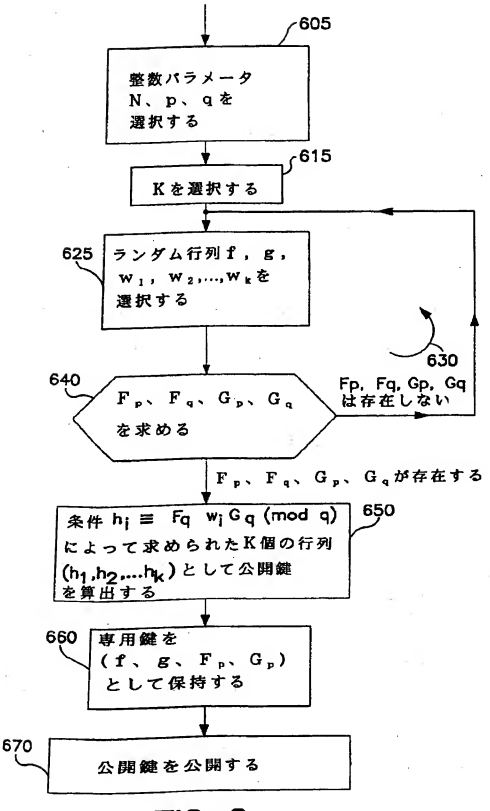

605
整数パラメータ
N、p、qを
選択する
615
Kを選択する
625
ランダム行列f，g，
w_1，w_2，…，w_kを
選択する
630
Fp, Fq, Gp, Gq
は存在しない
640
F_p、F_q、G_p、G_q
を求める
F_p、F_q、G_p、G_qが存在する
条件 $h_i \equiv F_q\ w_i G_q \pmod q$
によって求められたK個の行列
$(h_1, h_2, \ldots h_k)$として公開鍵
を算出する
650
660
専用鍵を
（f、g、F_p、G_p）
として保持する
670
公開鍵を公開する

FIG. 6

【図７】

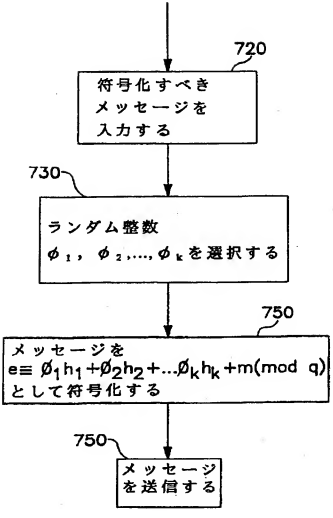

720
符号化すべき
メッセージを
入力する
730
ランダム整数
ϕ_1, ϕ_2,..., ϕ_kを選択する
750
メッセージを
$e \equiv \phi_1 h_1 + \phi_2 h_2 + \ldots \phi_k h_k + m \pmod q$
として符号化する
750
メッセージ
を送信する

FIG. 7

【図８】

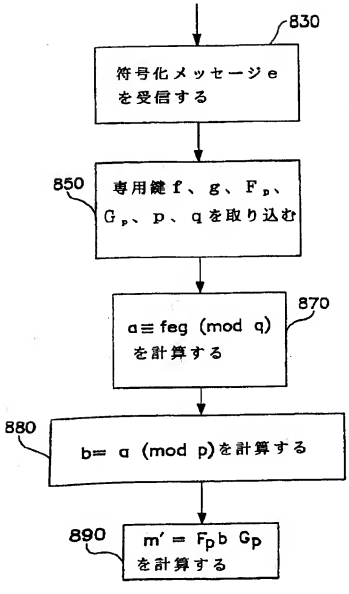

830
符号化メッセージｅを受信する
850
専用鍵ｆ、ｇ、F_p、G_p、ｐ、ｑを取り込む
870
a≡feg (mod q)を計算する
880
b≡ a (mod p)を計算する
890
m′ ≡ F_pb G_pを計算する

FIG. 8

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/15826

A. CLASSIFICATION OF SUBJECT MATTER
IPC(6) :H04K 1/00
US CL :380/30, 28, 49
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED
Minimum documentation searched (classification system followed by classification symbols)
U.S. : 380/30, 28, 49

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A, P	US 5,600,725 A (RUEPPEL et al.) 04 February 1997.	1-56
A, P	US 5,577,124 A (ANSHEL et al.) 19 November 1996.	1-56
A	US 5,375,170 A (SHAMIR) 20 December 1994.	1-56
A	US 5,351,297 A (MIYAJI et al.) 27 September 1994.	1-56

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"B" earlier document published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search
05 DECEMBER 1997

Date of mailing of the international search report
27 JAN 1998

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703) 305-3230

Authorized officer
DAVID CAIN
Telephone No. (703) 305-1836

Form PCT/ISA/210 (second sheet)(July 1992)*

フロントページの続き

(72)発明者 パイファー ジル
アメリカ合衆国，ロード アイランド
02860，ポータケット，レスター ウェイ，
３番地
(72)発明者 シルヴァーマン ジョセフ エイチ．
アメリカ合衆国，マサチューセッツ
02192，ニーダム，ノース ヒル アヴェ
ニュー，57番地